BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

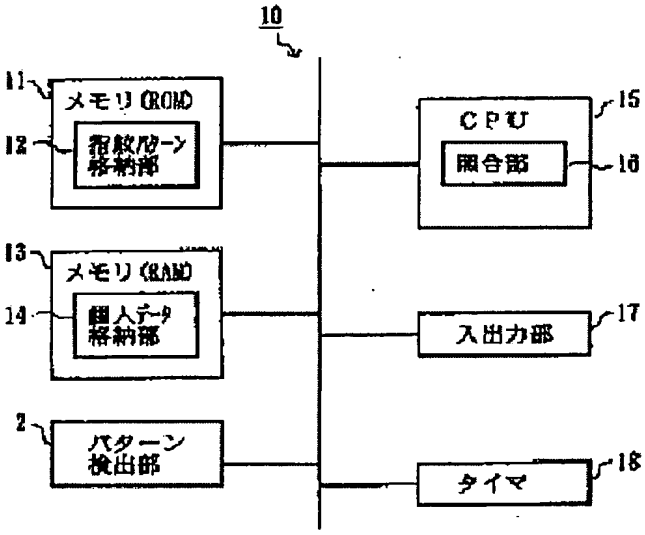
IC CARD AND DEVICE FOR INSERTING THE SAME

Patent number:	JP11184992
Publication date:	1999-07-09
Inventor:	YAMAKITA TORU
Applicant:	CASIO COMPUT CO LTD
Classification:	
- international:	G06K17/00; G06T7/00; G06K19/10; G06K19/07
- european:	
Application number:	JP19970354268 19971224
Priority number(s):	

Abstract of **JP11184992**

PROBLEM TO BE SOLVED: To attain improvement in security by judging whether an IC card is used by an authorized user or not while using a fingerprint pattern.

SOLUTION: A memory 11 is provided with a fingerprint pattern storage part 12 as a ROM area for storing the fingerprint pattern of a prescribed finger of the card user. A pattern detecting part 2 detects the rugged surface of an object pressed onto its surface. A collation part 16 of a CPU 15 is provided by executing one part of a program and collates the fingerprint pattern stored in the fingerprint pattern storage part 12 with the fingerprint pattern of the card user read by the pattern detecting part 2. Thus, the IC card itself judges whether a person to use the IC card is the authorized user or not and reports the judged result to a main body device. When the IC card is used by a person, who is not an authorized user (illegally used), the main body device inhibits processing based on that IC card.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－184992

(43)公開日　平成11年(1999)７月９日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00		Ｖ
				Ｂ
Ｇ０６Ｔ　7/00		Ｇ０６Ｆ　15/62		４６０
Ｇ０６Ｋ　19/10		Ｇ０６Ｋ　19/00		Ｓ
19/07				Ｊ

審査請求　未請求　請求項の数７　ＯＬ　（全 15 頁）

(21)出願番号　特願平9－354268

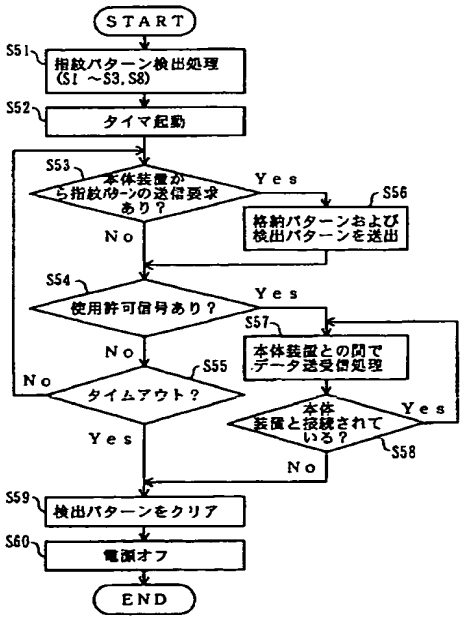
(22)出願日　平成９年(1997)12月24日

(71)出願人　000001443
カシオ計算機株式会社
東京都渋谷区本町１丁目６番２号
(72)発明者　山北　徹
東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内
(74)代理人　弁理士　阪本　紀康

(54)【発明の名称】　ＩＣカードおよびＩＣカードが挿入される装置

(57)【要約】
【課題】　使用者の負担を小さくしながら高いセキュリティが得られるＩＣカードおよびそのＩＣカードが挿入される装置を提供する。
【解決手段】　ＩＣカードは、使用者の指紋パターンを検出し、その検出した指紋パターンおよび予め格納してある指紋パターンを本体装置に送出する。本体装置は、これら２つの指紋パターンを照合し、一致した場合にはＩＣカードに対して使用許可信号を送信する。ＩＣカードは、使用許可信号を受信すると、本体装置との間でデータの送受信を行う。

第３の実施例のＩＣカードの処理のフローチャート



1

【特許請求の範囲】
【請求項１】　物体の表面のパターンを検出する検出手段と、
指紋パターンを格納する格納手段と、
上記検出手段により検出された指紋パターンと上記格納手段に格納されている指紋パターンとを照合し、その照合結果を出力する照合手段と、を有し、
上記照合手段が出力する照合結果に基づいて処理を許可するか否かを判断する装置に挿入されるＩＣカード。
【請求項２】　上記照合手段は、上記照合結果を所定期間出力する請求項１に記載のＩＣカード。
【請求項３】　物体の表面のパターンを検出する検出手段と、
指紋パターンを格納する格納手段と、
上記検出手段により検出された指紋パターンおよび上記格納手段に格納されている指紋パターンを出力する出力手段と、を有し、
上記出力手段が出力する各指紋パターンを照合して処理を許可するか否かを判断する装置に挿入されるＩＣカード。
【請求項４】　ＩＣカードが挿入される装置であって、
上記ＩＣカードに予め格納されている指紋パターンとそのＩＣカードが検出した指紋パターンとの照合結果として、それら２つの指紋パターンが互いに一致している旨の通知をそのＩＣカードから受信した際に、そのＩＣカードに基づく処理を許可する装置。
【請求項５】　上記ＩＣカードが、照合結果として、上記２つの指紋パターン間の類似度を複数段階で評価した結果を出力した場合、
類似度の段階に応じて、
そのＩＣカードに基づく処理を許可し、
もしくは、使用者にパスワードを要求してその要求に対して正規のパスワードが入力された場合にそのＩＣカードに基づく処理を許可し、
もしくは、そのＩＣカードに基づく処理を禁止する、
請求項４に記載の装置。
【請求項６】　ＩＣカードが挿入される装置であって、
上記ＩＣカードに予め格納されている指紋パターンおよびそのＩＣカードが検出した指紋パターンをそのＩＣカードから受信する受信手段と、
上記２つの指紋パターンを照合し、それらが互いに一致していた場合にそのＩＣカードに基づく処理を許可する照合手段と、
を有する装置。
【請求項７】　上記照合手段は、上記２つの指紋パターン間の類似度を複数段階で評価し、類似度の段階に応じて、
そのＩＣカードに基づく処理を許可し、
もしくは、使用者にパスワードを要求してその要求に対して正規のパスワードが入力された場合にそのＩＣカードに基づく処理を許可し、
もしくは、そのＩＣカードに基づく処理を禁止する、
請求項６に記載の装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ＩＣカード、および挿入されたＩＣカードとの間でデータを送信または受信する装置に係わる。
【０００２】
【従来の技術】従来から、使用する者の身分証明（ＩＤ）としての機能が電子的に組み込まれたカードが広く普及している。たとえば、銀行等の口座にアクセスするための、いわゆるキャッシュカードやクレジットカード、あるいはドアのロックを解除したり、各種装置を起動するためのＩＤカードなどである。これらのカードには、通常、そのカードの使用者を識別する情報が書き込まれた磁気フィルム等が貼り付けられている。そして、使用時には、そのカードが挿入された装置がその識別情報を読み取り、アクセス等の処理を許可するか否かなどを判断する。
【０００３】ところが、上述のような単純な方式だと、カードを紛失した場合などには、それを拾った他人が不正にそのカードを使用できることになる。そこで、キャッシュカード等においては、上述のような磁気フィルム等に書き込まれた識別情報と共に、暗証番号（パスワード）が併用されることが一般的である。例えば、キャッシュカードが挿入されると、ユーザに暗証番号を要求し、その要求に対して予め登録されている正規の暗証番号が投入されたときにのみアクセスを許可するようなシステムは広く実施されている。
【０００４】また、近年、上述のようなカードにインテリジェントな機能を持たせるために集積回路を組み込んだカード型の機器（通常、ＩＣカードと呼ばれることが多いので、以下、そのように呼ぶことにする）の研究・開発が盛んである。ＩＣカードは、将来、電子マネーや電子財布の分野においてその中心的な役割を担うことが予想されているので、特に、他人の不正使用を防ぐために高いセキュリティを確保することが必須の要件となっている。
【０００５】
【発明が解決しようとする課題】現在、他人による各種カード類（ＩＣカードを含む）の不正使用を防ぐ手法としては、暗証番号（パスワード）が最も一般的である。ところが、この場合、各カード使用者は、暗証番号を覚えておく必要があり、特に所持するカードの枚数が多いとその負担が大きくなっていた。また、暗証番号は、流出してしまう恐れがあった。
【０００６】本発明の課題は、上述の問題を解決することであり、使用者の負担を小さくしながら高いセキュリティが得られるＩＣカードおよびそのＩＣカードが挿入

2

される装置を提供することである。

【０００７】

【課題を解決するための手段】本発明のＩＣカードは、物体の表面のパターンを検出する検出手段と、指紋パターンを格納する格納手段と、上記検出手段により検出された指紋パターンと上記格納手段に格納されている指紋パターンとを照合し、その照合結果を出力する照合手段と、を有する。

【０００８】上記ＩＣカードが挿入される装置は、そのＩＣカードに予め格納されている指紋パターンとそのＩＣカードが検出した指紋パターンとの照合結果としてそれら２つの指紋パターンが互いに一致している旨の通知をそのＩＣカードから受信した際に、そのＩＣカードに基づく処理を許可する構成である。

【０００９】上記構成によれば、格納手段に格納されている指紋パターンを持つ者以外の者がこのＩＣカードを使用すると、照合手段による照合結果は不一致となる。したがって、上記ＩＣカードが挿入される装置は、そのＩＣカードに基づく処理を禁止する。このようにして、指紋パターンにより不正使用を防ぐ。

【００１０】本発明の他の形態のＩＣカードは、物体の表面のパターンを検出する検出手段と、指紋パターンを格納する格納手段と、上記検出手段により検出された指紋パターンおよび上記格納手段に格納されている指紋パターンを出力する出力手段とを有する。

【００１１】上記他の形態のＩＣカードが挿入される装置は、そのＩＣカードに予め格納されている指紋パターンおよびそのＩＣカードが検出した指紋パターンをそのＩＣカードから受信する受信手段と、上記２つの指紋パターンを照合し、それらが互いに一致していた場合にそのＩＣカードに基づく処理を許可する照合手段と、を有する構成である。この形態の作用は、上述した作用と同じである。

【００１２】

【発明の実施の形態】以下、本発明の実施形態について図面を参照しながら説明する。図１(a) および(b) は、本実施形態のＩＣカードの外観図である。ＩＣカード１は、たとえば、銀行口座へのアクセス、商品購入時の支払い、ドアロックの解除、あるいは各種装置の起動などに際して使用されるカード型の機器である。ＩＣカード１は、その表面の一部に、パターン検出部２が設けられている。パターン検出部２は、そこに接触された物体の表面のパターン（凹凸パターン等）を検出する機能を有し、本実施形態では、カード使用者の指紋パターンを読み取るために使用される。

【００１３】カード使用者は、ＩＣカード１を使用する際には、まず、スイッチをオンにした後、予め決めてある所定の指をパターン検出部２に押圧する。図１(a) に示す例では、右手の人差し指をパターン検出部２に押圧する例を示している。所定の指をパターン検出部２に押圧するときには、指紋パターンが確実に検出されるように、親指を使ってＩＣカード１を挟み付けるようにすることが望ましい（図１(b) 参照）。

【００１４】ＩＣカード１には、その使用者の所定の指（図１に示す実施例では、右手の人差し指）の指紋パターンが予め格納されている。そして、後述する第１および第２の実施例では、ＩＣカード１は、その予め格納されている指紋パターンとパターン検出部２により検出された指紋パターンとを照合し、その照合結果を出力する。また、第３の実施例では、ＩＣカード１は、そのカードが挿入される本体装置に対して、上記予め格納されている指紋パターンおよびパターン検出部２により検出された指紋パターンを出力し、その本体装置がそれらの指紋パターンを照合する。そして、本体装置は、各実施例において、上記２つの指紋パターンが一致したときに、ＩＣカード１に基づく処理（ＩＣカード１を用いたアクセスを含む）を許可し、以降、その間でデータを送受信する。

第１の実施例

第１の実施例は、ＩＣカードに指紋照合機能を持たせた構成である。

【００１５】図２は、第１（および第２）の実施例のＩＣカード１０の構成図である。メモリ１１は、ＲＯＭ領域であり、カード使用者の所定の指の指紋パターンを格納するための指紋パターン格納部１２を含む。この指紋パターンは、たとえば、カードの発行時に格納される。メモリ１１には、後述するフローチャートの処理を記述したプログラム等も格納されている。メモリ１３は、ＲＡＭ領域であり、上記プログラムを実行する際に使用される領域の他、カード使用者の個人情報を格納する個人データ格納部１４が設けられている。個人データ格納部１４は、たとえば、このＩＣカード１０が電子マネーシステムにおける電子財布であったとすると、「財布の中の金額」に相当する情報などを格納する。なお、個人データ格納部１４は、不揮発性メモリ領域に設けられる。

【００１６】パターン検出部２は、その表面に押圧された物体の表面の凹凸を検出する装置であり、微細化技術の進歩によりＩＣカードに組み込むことができる程度に薄く形成されている。パターン検出部２は、たとえば、光源および２次元フォトセンサを含み、その２次元フォトセンサを構成する多数の受光素子がそれぞれ検出する受光レベルに対応する電流値または電圧値をシリアル形式またはパラレル形式で出力する。なお、本発明の出願人は、先に、十分に薄型でありながら高い精度で物体の表面の凹凸パターンを検出することができる読取装置について特許出願をしている（特願平９－２２２０１８号）。

【００１７】ＣＰＵ１５は、メモリ１１に格納されているプログラムを実行する。ＣＰＵ１５は、照合部１６を備える。照合部１６は、上記プログラムの一部を実行す

ることにより実現され、指紋パターン格納部１２に格納されている指紋パターンとパターン検出部２により読み取られたカード使用者の指紋パターンとを照合する。入出力部１７は、このＩＣカード１０が挿入される本体装置との間でデータを送受信する。タイマ１８は、ＣＰＵ１５により起動され、所定時間が経過するとＣＰＵ１５に割込信号を送出する。

【００１８】図３は、第１（および第２）の実施例の本体装置２０の構成図である。この本体装置２０には、図２に示したＩＣカード１０が挿入される。ＩＣカード１０は、カード挿入部２１に挿入される。カード挿入部２１は、ＩＣカード１０とのインタフェースをとるためのＩ／Ｆ部２２を備える。ＣＰＵ２３は、メモリ２４に格納されているプログラムを実行することにより、ＩＣカード１０とのデータの授受、また、必要に応じて不図示の外部装置（ホストコンピュータなど）とのデータの授受を制御する。メモリ２４は、後述するフローチャートの処理を始め、この本体装置２０の各ソフトウェア処理を記述したプログラムおよびこの本体装置２０が使用する各種データを格納する。なお、ここでは、カード挿入部２１、ＣＰＵ２３およびメモリ２４が１つの装置の中に設けられているように記載しているが、これらを互いに異なる場所に設け、通信回線等を用いた互いに接続する構成であってもよい。

【００１９】図４および図５は、第１の実施例におけるＩＣカードの処理のフローチャートである。この処理は、ＩＣカードの電源をオンにしたことをトリガとして実行される。

【００２０】ステップＳ１では、電源がオンにされたときから一定時間内にパターン検出部２に入力があったか否かを調べる。この処理は、たとえば、パターン検出部２の出力が変化したか否かを調べるものである。パターン検出部２に入力があった場合には、ユーザが所望の指の指先（指紋が形成されている部分）をパターン検出部５に押圧したものと見なし、ステップＳ２へ進み、一方、入力が無かった場合には、ステップＳ８においてＩＣカードの電源をオフにする。

【００２１】ステップＳ２では、指紋パターンを検出する。すなわち、パターン検出部２の出力を取り込む。この指紋パターンは、たとえば、メモリ１３の所定の領域に保持される。ステップＳ３では、指紋パターンを適切に検出できたか否かを判断する。すなわち、ユーザの指がパターン検出部２に一定時間以上固定されなかった場合や、押圧が弱く接触面積が小さかった場合などには、指紋パターンを再生できないので、このステップで指紋パターンを適切に検出できたか否かを判断している。指紋パターンを適切に検出できた場合には、ステップＳ４へ進み、検出できなかった場合にはステップＳ１へ戻る。

【００２２】ステップＳ４では、指紋パターン格納部１２に格納されている指紋パターンとパターン検出部２により検出された指紋パターンとを照合する。この処理は、例えば、上記２つの指紋パターンの類似度を数値化する手順を含む。

【００２３】ステップＳ５では、上記ステップＳ４により得られた類似度を表す値が、予め設定してある閾値を越えるか否かに従って「一致／不一致」を判断する。上記２つの指紋パターンが互いに一致していた場合には、ステップＳ６において、ＯＫ信号を出力する。この処理は、例えば、このＩＣカードが挿入される本体装置２０のＩ／Ｆ部２２と接触する端子の中の所定の１つを「Ｌ」レベルから「Ｈ」レベルに切り換えるものである。ステップＳ７では、タイマ１８を起動する。

【００２４】ステップＳ１１およびＳ１２では、使用許可信号を受信しているか否かを調べる。なお、この使用許可信号は、後述説明するが、図４に示した本体装置２０により生成される信号であり、本体装置２０がそこに挿入されたＩＣカードに基づく処理を許可すると判断した際に本体装置２０によって出力される。ここで、タイマ１８に設定されている所定の時間が経過する前に使用許可信号を受信した場合には、ステップＳ１６およびＳ１７において、本体装置２０との間でデータを送受信する処理を実行する。この処理は、ＩＣカードが本体装置２０と接続されている間は継続される。

【００２５】本体装置２０がこのＩＣカードを排出するなどして本体装置２０との接続が終了すると、ステップＳ１３へ進んでＯＫ信号をリセットする。すなわち、ＯＫ信号の送出を停止する。続いて、ステップＳ１４では、ステップＳ２においてパターン検出部２により検出した指紋パターンをクリアする。そして、ステップＳ１５において、このＩＣカードの電源をオフにする。

【００２６】一方、ステップＳ１１およびＳ１２において、タイマ１８に設定されている所定の時間が経過するまでに使用許可信号を受信できなかった場合、すなわち、タイマ１８がタイムアウトした場合には、ステップＳ１６およびＳ１７を実行することなくステップＳ１３へ進む。すなわち、本体装置２０から使用許可信号を受信できなかった場合には、このＩＣカードは、本体装置２０との間でデータを授受できない。

【００２７】なお、ステップＳ５において、指紋パターン格納部１２に格納されている指紋パターンとパターン検出部２により検出された指紋パターンとが一致しないと判断した場合には、ＯＫ信号を出力することなくステップＳ１４へジャンプし、その検出した指紋パターンをクリアした後に電源をオフにする。

【００２８】図６は、第１の実施例における本体装置の処理のフローチャートである。この処理は、ＩＣカード１０が挿入されたことをトリガとして実行される。ステップＳ２１およびＳ２２では、ＩＣカード１０が挿入されたときから一定時間内にそのＩＣカード１０からＯＫ

信号を受信したか否かを調べる。ＯＫ信号は、上述したように、指紋パターン格納部１２に格納されている指紋パターンとパターン検出部２により検出された指紋パターンとが一致した場合にＩＣカード１０により出力される信号である。ＯＫ信号を受信した場合には、ステップＳ２３へ進み、一方、受信できなかった場合には、ステップＳ２５において挿入されたＩＣカード１０を排出する。

【００２９】ステップＳ２３では、ＩＣカード１０へ使用許可信号を送出する。この使用許可信号は、図５のステップＳ１１およびＳ１２において監視される信号であり、ＩＣカード１０は、この信号を受信すると、この本体装置とデータを授受できる状態になる。ステップＳ２４では、ＩＣカード１０との間でデータを送受信する処理を実行する。なお、上述したＯＫ信号は、ＩＣカードの正規の使用者（所有者）とそのＩＣカードに指紋を読み取らせた者とが一致しているか否かを表す情報なので、そのＩＣカードの使用者を識別する情報はこのステップＳ２４において受信する。したがって、もし、そのＩＣカードの使用者を識別する情報が正規に登録されていなかった場合などには、ＯＫ信号を受信した場合であってもそのＩＣカードに基づく処理を拒絶することがある。また、この本体装置が、ＩＣカード１０とのデータの授受に際して不図示のホストコンピュータなどとの間でデータを授受する必要がある場合には、その処理はステップＳ２４と並列に実行される。

【００３０】このように、第１の実施例では、ＩＣカードを使用する者が正規の使用者であるか否かをＩＣカード自身が判断し、その判断結果を本体装置に通知する。そして、本体装置は、正規の使用者でない者の使用（すなわち、不正使用）であった場合には、そのＩＣカードに基づく処理を禁止する。

第２の実施例

第２の実施例は、第１の実施例の構成に加え、指紋パターンの一致／不一致の判断が微妙な時に、使用者にパスワードを要求する機能を設けた構成である。なお、第２の実施例におけるＩＣカードおよび本体装置の構成は、第１の実施例と同じであり、それぞれ図２および図３に示した通りである。

【００３１】近年では、画像認識技術が進歩してきてはいるが、一般に、パターンマッチング処理の精度は１００パーセントではない。そして、この精度は、プロセッサの能力が低い場合や、短時間で処理しなければならない状況においては、低下するものと予想される。したがって、カードを使用する者が正規の使用者であるか否かの判断は、第１の実施例において述べたように、指紋パターンの類似度を数値化してその値が所定の閾値よりも大きいか否かに基づいて決定する方式が現実的である。ところが、この閾値の設定は難しく、一致／不一致の判断を甘くすれば不正使用を排除できない恐れがあり、反対に、その判断を厳密にすれば、正規の使用者が使用しているにも係わらずその正規の使用者によるアクセスを拒絶してしまうことも起こりかねない。

【００３２】そこで、第２の実施例では、ＩＣカードは、指紋パターンの類似度を複数段階で評価し、ＩＣカードに基づく処理を許可するか否かに際して、きめ細かい判断をできるようにした。具体的には、指紋パターンの類似度を、「非常に高い」、「比較的高い」および「低い」の３段階で評価して出力し、本体装置は、「類似度が非常に高い」を受信したときには、そのまま処理を許可するが、「類似度が比較的高い」を受信したときには、使用者にパスワードを要求する。

【００３３】図７は、第２の実施例におけるＩＣカードの処理のフローチャートである。この処理は、第１の実施例と同様に、ＩＣカードの電源をオンにしたことをトリガとして実行される。なお、図７において、照合処理（ステップＳ７）、タイマ起動処理（ステップＳ７）、クリア処理（ステップＳ１４）、電源オフ処理（ステップＳ１５）は、第１の実施例と同じである。

【００３４】ステップＳ３１では、パターン検出部２により指紋パターンを検出する。この処理は、第１の実施例のステップＳ１～Ｓ３およびＳ８と同じである。続いて、ステップＳ４において、指紋パターン格納部１２に格納されている指紋パターンとパターン検出部２により検出された指紋パターンとを照合し、その類似度を数値化する。

【００３５】ステップＳ３２では、ステップＳ４で得られた類似度が、「非常に高い」に属するか否かを調べる。類似度が非常に高ければ、ステップＳ３３においてＯＫ１信号を出力し、そうでなければ、ステップＳ３４へ進む。ステップＳ３４では、ステップＳ４で得られた類似度が、「比較的高い」に属するか否かを調べる。類似度が比較的高ければ、ステップＳ３５においてＯＫ２信号を出力する。ＯＫ１信号またはＯＫ２信号を出力した場合には、ステップＳ７において、タイマ１８を起動する。

【００３６】ステップＳ３６は、使用許可信号を監視する処理、および使用許可信号を受信した場合に本体装置との間でデータを送受信する処理である。これらの処理は、第１の実施例のステップＳ１１、Ｓ１２、Ｓ１６およびＳ１７と同じである。ステップＳ３７では、ＯＫ１信号またはＯＫ２信号をリセットする。即ち、ＯＫ１信号またはＯＫ２信号の出力を停止する。なお、これらの信号をリセットする処理は、タイマ１８のタイムアウトした場合、あるいは本体装置から使用許可信号を受信した場合に実行される。この後、ステップＳ１４およびＳ１５において、パターン検出部２により検出したパターンをクリアし、ＩＣカードの電源をオフにする。

【００３７】なお、ステップＳ４で得られた類似度が低いと判断した場合（ステップＳ３２：Ｎｏ、且つステッ

ブＳ３４：Ｎｏ）には、正規の使用者でない者がこのＩＣカードを使用しているものとみなし、ＯＫ１信号またはＯＫ２信号のいずれも出力することなく、ステップＳ１４へジャンプする。

【００３８】図８は、第２の実施例における本体装置の処理のフローチャートである。この処理は、第１の実施例と同様に、ＩＣカードが挿入されたことをトリガとして実行される。

【００３９】ステップＳ４１～Ｓ４３は、挿入されたＩＣカードから所定時間内にＯＫ１信号またはＯＫ２信号を受信したか否かを監視する処理である。ＯＫ１信号を受信した場合、すなわちＩＣカードにおいて照合された２つの指紋パターンの類似度が非常に高い旨の通知を受けた場合には、そのＩＣカードを使用している者が正規の使用者であるとみなし、ステップＳ２３において使用許可信号を送出する。そして、ステップＳ２４において、ＩＣカードとの間でデータを送受信する処理を実行する。これらのステップＳ２３およびＳ２４は、第１の実施例における処理と同じである。

【００４０】ＯＫ信号２を受信した場合、すなわちＩＣカードにおいて照合された２つの指紋パターンの類似度が比較的高い旨の通知を受けた場合には、そのＩＣカードを使用している者が正規の使用者である可能性が高いもののそうでない可能性もあるとみなし、ステップＳ４４においてパスワードを要求する。続いて、ステップＳ４５では、まず、その挿入されたＩＣカードを識別する情報をそのＩＣカードから読み取り、その識別情報に対して予め登録されているパスワードを抽出しておく。そして、上記要求に応答してカード使用者により入力されたパスワードとその予め登録されているパスワードとを照合する。ステップＳ４６では、ステップＳ４５における照合の結果を判断し、パスワードが一致していればステップＳ２３へ進んで、使用許可信号を送出する処理、およびＩＣカードとの間でデータを送受信する処理を実行し、一致していなければ、これらの処理をスキップしてステップＳ２５へ進む。

【００４１】所定時間内にＯＫ１信号またはＯＫ２信号のいずれも受信できなかった場合には、ＩＣカードを使用している者が正規の使用者ではないとみなし、使用許可信号を送出することなくそのＩＣカードを排出する。

【００４２】このように、第２の実施例では、指紋パターンの照合結果のみではＩＣカードを使用している者が正規の使用者であるのか否かを判断できない場合に、使用者にパスワードを入力させる構成を導入した。この結果、正しいパスワードを知らない不正使用者を確実に排除できると共に、正規の使用者が使用できないような状況は回避される。また、パスワードを併用するので、指紋パターンの照合の精度がさほど高くなくてもＩＣカードを使用する者が正規の使用者であるか否かを判断できる。したがって、ＩＣカード内に設けるＣＰＵの性能はさほど高くなくてもよく、ＩＣカードの自体のコストアップを抑えられる。

第３の実施例

第３実施例は、指紋パターンを照合する処理をＩＣカードが挿入される本体装置において実行する構成である。

【００４３】図９は、第３の実施例のＩＣカードの構成図である。第３の実施例のＩＣカードは、基本的には第１または第２の実施例と同じ構成であるが、指紋パターンを照合する処理を実行しないので、照合部１６は設けられていない。

【００４４】図１０は、第３の実施例の本体装置の構成図である。第３の実施例の本体装置は、基本的には第１または第２の実施例と同じ構成であるが、指紋パターンを照合する処理を実行する。このため、ＣＰＵ３１がメモリ２４に格納されているプログラムを実行することによって得られる機能の一部として照合部３１が設けられている。

【００４５】図１１は、第３の実施例におけるＩＣカードの処理のフローチャートである。この処理は、第１または第２の実施例と同様に、ＩＣカードの電源をオンにしたことをトリガとして実行される。

【００４６】ステップＳ５１では、パターン検出部２により指紋パターンを検出する。この処理は、第１の実施例のステップＳ１～Ｓ３およびＳ８と同じである。続いて、ステップＳ５２では、タイマ１８を起動する。

【００４７】ステップＳ５３～５５は、タイマ１８がタイムアウトする前に、このＩＣカードが挿入された本体装置から指紋パターンの送信要求を受信したか否か、および使用許可信号を受信したか否かを調べる処理である。本体装置から指紋パターンの送信要求を受信した場合には、ステップＳ５６において、指紋パターン格納部１２に格納されている指紋パターンおよびパターン検出部２により検出した指紋パターンを本体装置へ送出する。また、使用許可信号を受信した場合には、ステップＳ５７およびＳ５８において、本体装置との間でデータを送受信する処理を実行する。この処理は、このＩＣカードが本体装置と接続されている間は継続される。

【００４８】本体装置から使用許可信号を受信することなくタイマ１８がタイムアウトした場合、または本体装置との接続が終了した場合には、パターン検出部２により検出した検出パターンをステップＳ５９においてクリアし、ステップＳ６０においてこのＩＣカードの電源をオフにする。

【００４９】このように、第３の実施例のＩＣカードは、本体装置からの要求に応じて予め格納してある指紋パターンおよび検出した指紋パターンを送出する。本体装置はそれらの指紋パターンに基づいて使用を許可するか否かを判断する。そして、ＩＣカードは、本体装置から使用許可が与えられたときにのみ本体装置との間でデータの送受信が可能となる。

【００５０】図１２は、第３の実施例における本体装置の処理のフローチャートである。この処理は、第１または第２の実施例と同様に、ＩＣカードが挿入されたことをトリガとして実行される。

【００５１】ステップＳ６１～Ｓ６３は、挿入されたＩＣカードに対して指紋パターンの送出を要求し、所定時間内にその要求に応じて指紋パターンを受信できるか否かを判断する処理である。ＩＣカードから指紋パターンを受信した場合にはステップＳ６４へ進み、受信できなかった場合には、ステップＳ６８においてそのＩＣカードを排出する。

【００５２】ステップＳ６４では、ＩＣカードから受信した２つの指紋パターン、即ち指紋パターン格納部１２に格納されている指紋パターンおよびパターン検出部２により検出した指紋パターンを照合する。この処理は、たとえば、図４のステップＳ４の処理と同じであり、類似度を数値化する手順を含む。ステップＳ６５は、ステップＳ６４における照合処理の結果を参照し、上記２つの指紋が一致するのか否かを判断する。一致する場合には、ステップＳ６６においてＩＣカードに対して使用許可信号を送出し、ステップＳ６７においてそのＩＣカードとの間でデータの送受信処理を実行する。一方、上記２つの指紋が互いに一致しなかった場合は、ステップＳ６６およびＳ６７をスキップしてステップＳ６８へ進んでＩＣカードを排出する。

【００５３】このように、第３の実施例の本体装置は、挿入されたＩＣカードから予め格納してある指紋パターンおよび検出した指紋パターンを受信し、それらの指紋パターンが互いに一致した場合にのみＩＣカードに使用許可を与える。

【００５４】なお、第３の実施例においても、上述の第２の実施例と同様に、指紋パターンの照合とパスワードとを併用する構成としてもよい。このように、第３の実施例では、ＩＣカードにおいて指紋パターンの照合処理を実行しないので、ＩＣカードに設けるＣＰＵは高い性能を持つ必要がない。したがって、ＩＣカードの製造コストを低く抑えることができる。

【００５５】なお、上記第１～第３の実施例では、各ＩＣカードに１人の使用者の指紋パターンを予め格納しておく構成を示したが、本発明は、この形態に限定されるものではない。たとえば、家族や特定のグループの人間がＩＣカードを共有できるようにしてもよい。この場

合、ＩＣカードに予め複数人の指紋パターンを登録しておき、検出した指紋パターンとそれら複数の指紋パターンとを１つずつ照合してゆけばよい。

【００５６】

【発明の効果】ＩＣカードが正規の使用者により使用されているのか否かの判断を指紋パターンを用いて行うので、セキュリティが高い。このとき、カード使用者は、従来のようにパスワード等を覚えておく必要はなく、また、パスワード等の流出の恐れもない。さらに、ＩＣカードを使用する際の操作も簡単である。

【図面の簡単な説明】

【図１】本実施形態のＩＣカードの外観図である。

【図２】第１および第２の実施例のＩＣカードの構成図である。

【図３】第１および第２の実施例の本体装置の構成図である。

【図４】第１の実施例のＩＣカードの処理のフローチャート（その１）である。

【図５】第１の実施例のＩＣカードの処理のフローチャート（その２）である。

【図６】第１の実施例の本体装置の処理のフローチャートである。

【図７】第２の実施例のＩＣカードの処理のフローチャートである。

【図８】第２の実施例の本体装置の処理のフローチャートである。

【図９】第３の実施例のＩＣカードの構成図である。

【図１０】第３の実施例の本体装置の構成図である。

【図１１】第３の実施例のＩＣカードの処理のフローチャートである。

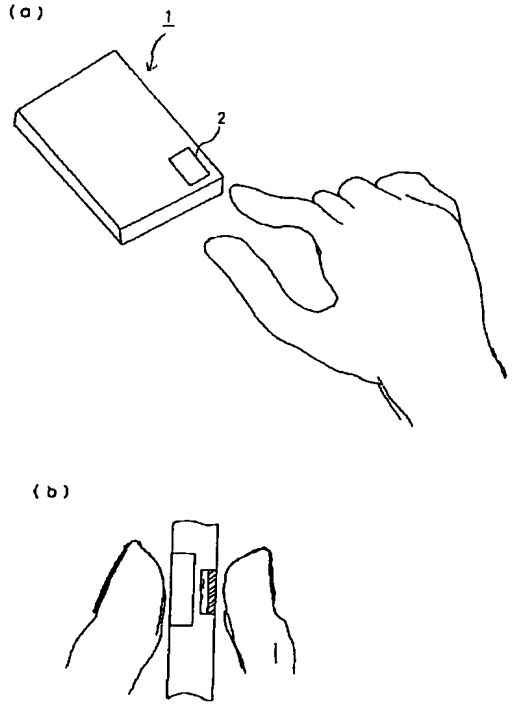
【図１２】第３の実施例の本体装置の処理のフローチャートである。

【符号の説明】

１	ＩＣカード
２	パターン検出部
１１、１３、２４	メモリ
１２	指紋パターン格納部
１５、２３	ＣＰＵ
１６、３１	照合部
１８	タイマ
２１	カード挿入部
２２	Ｉ／Ｆ部

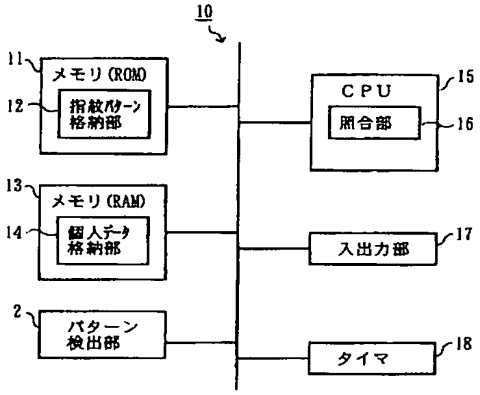
【図１】

本実施形態のＩＣカードの外観図



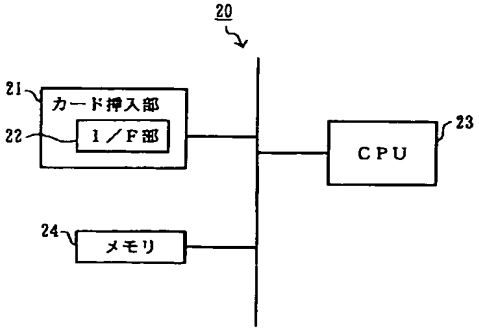
【図２】

第１および第２の実施例のＩＣカードの構成図



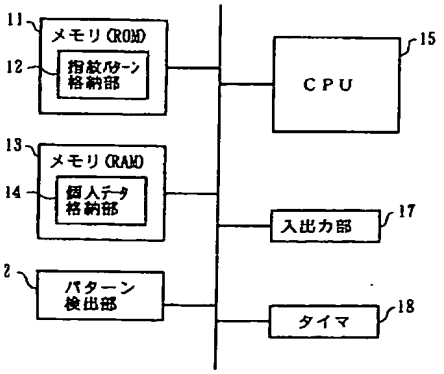
【図３】

第１および第２の実施例の本体装置の構成図



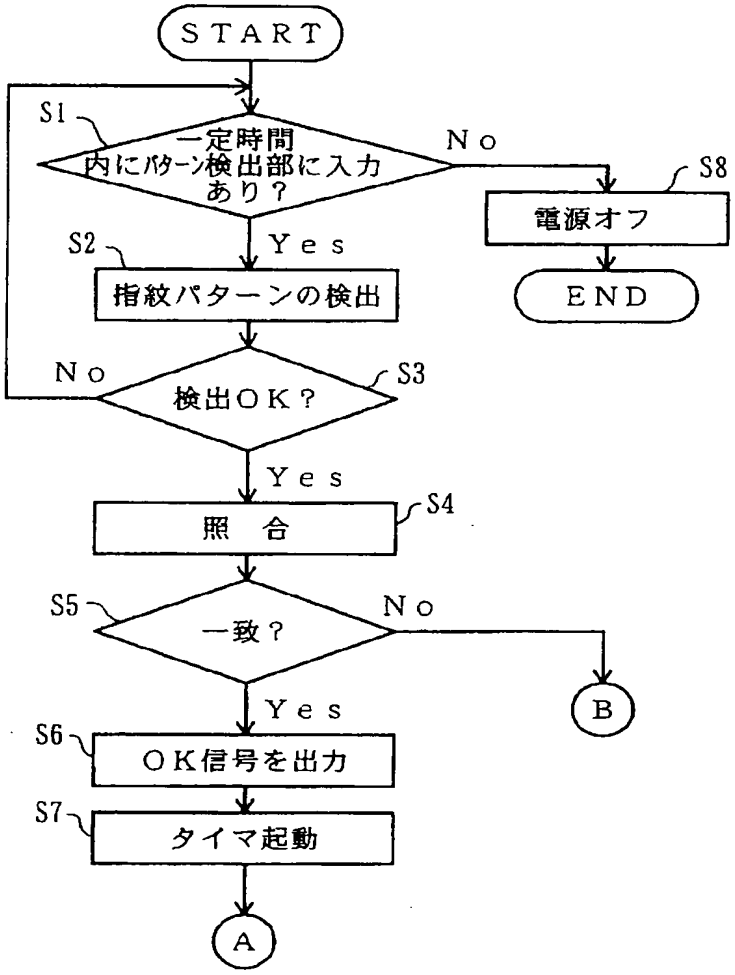
【図９】

第３の実施例のＩＣカードの構成図



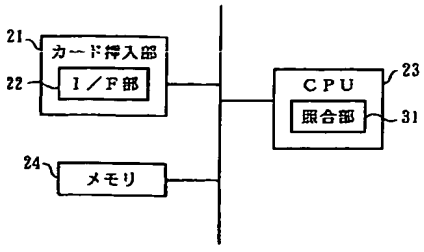
【図４】

第１の実施例のＩＣカードの処理のフローチャート（その１）



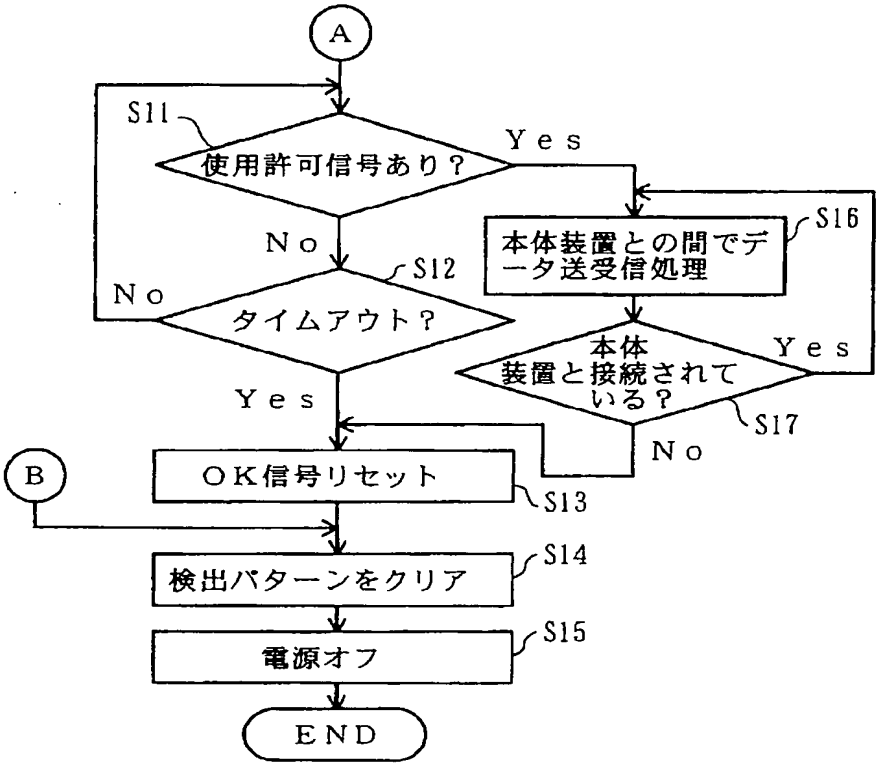
【図１０】

第３の実施例の本体装置の構成図



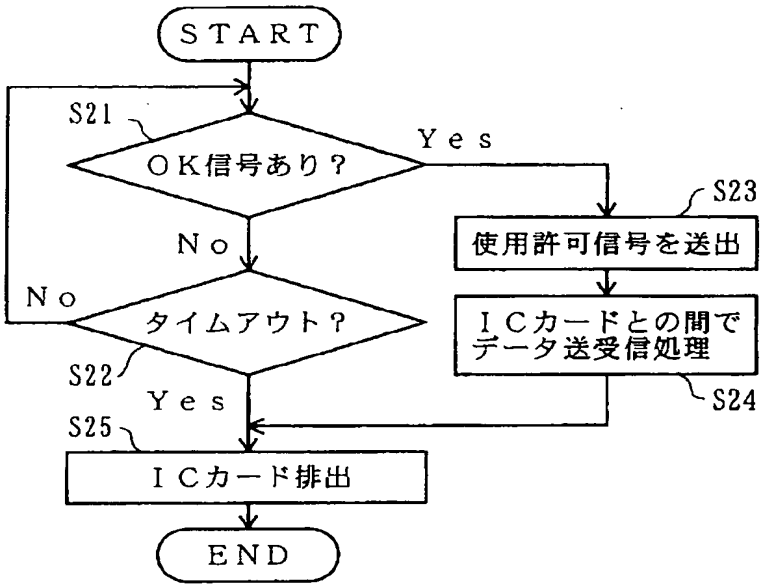
【図５】

第１の実施例のＩＣカードの処理のフローチャート（その２）



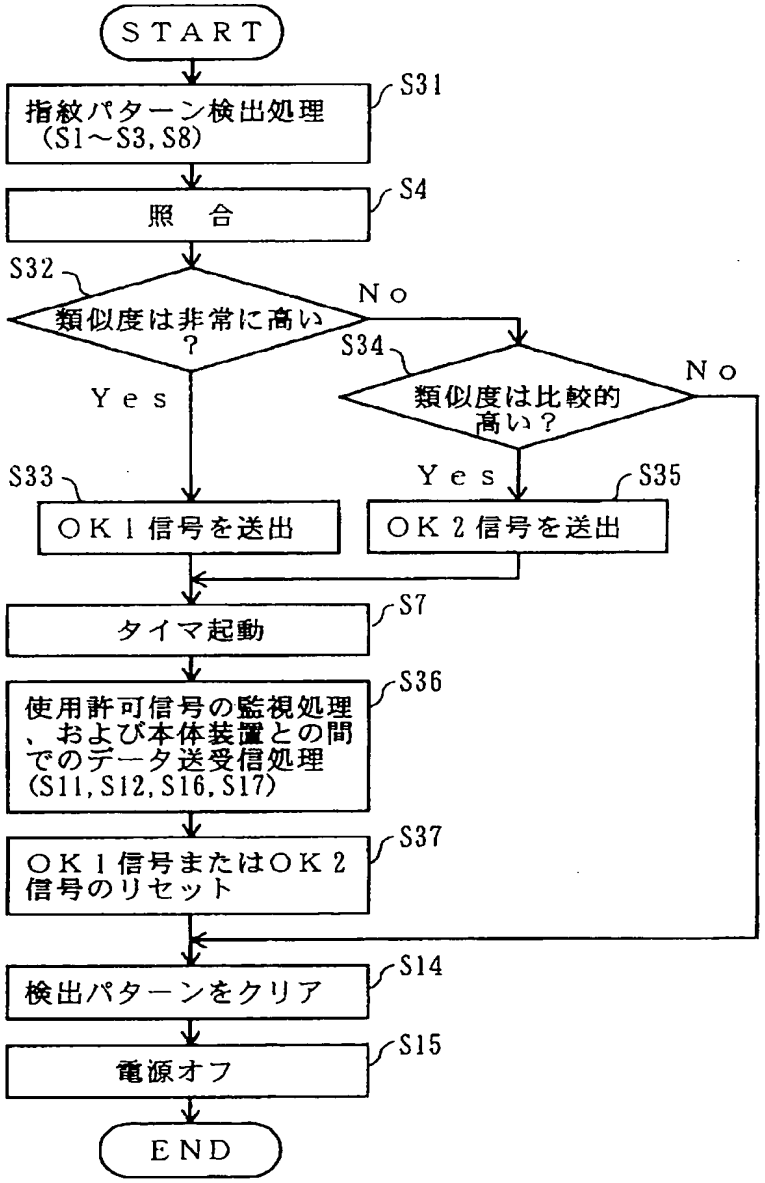
【図６】

第１の実施例の本体装置の処理のフローチャート



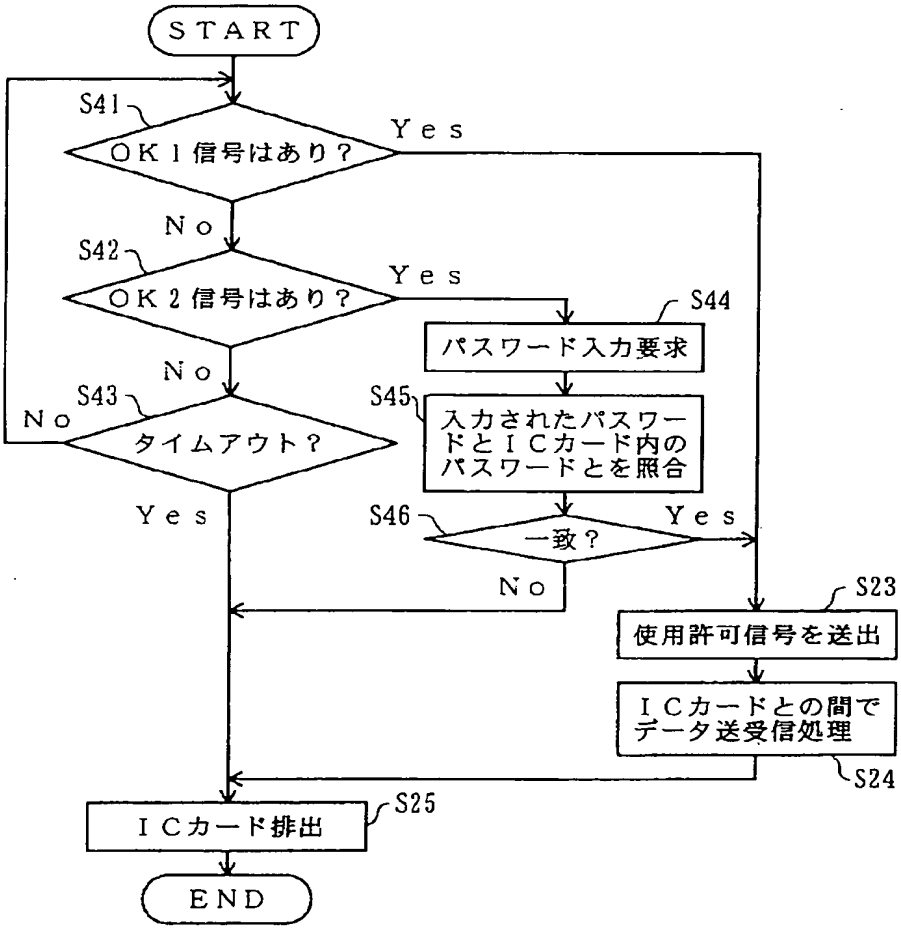
【図７】

第２の実施例のＩＣカードの処理のフローチャート



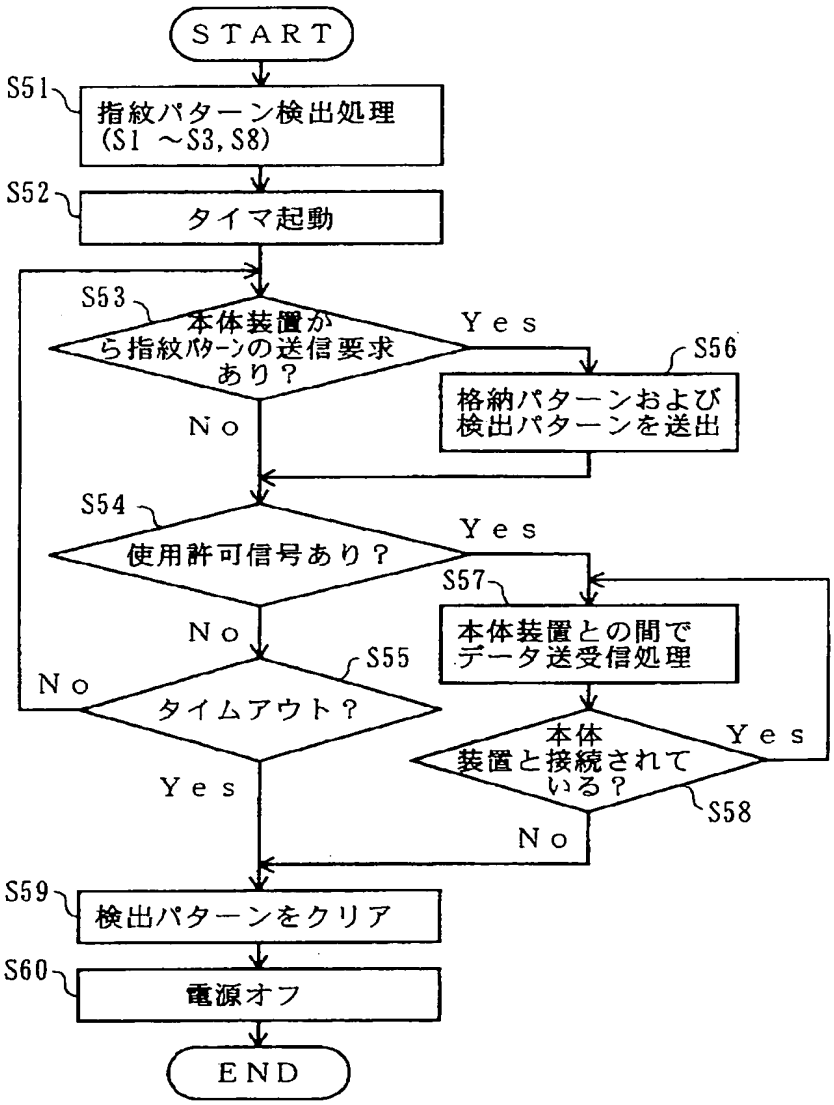
【図８】

第２の実施例の本体装置の処理のフローチャート



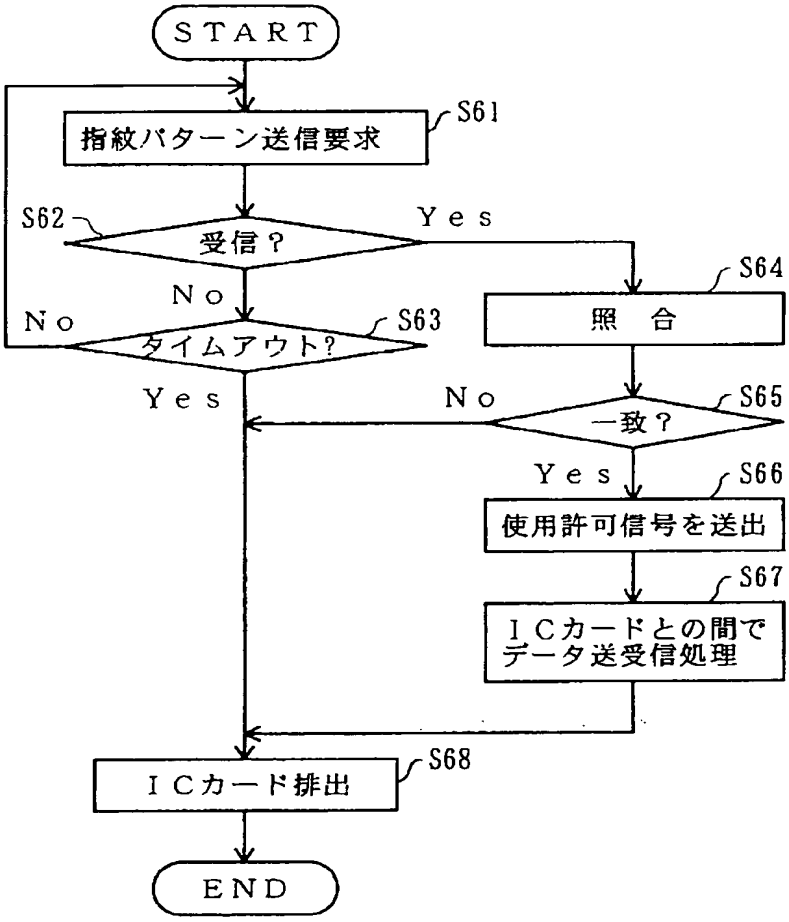
【図１１】

第３の実施例のＩＣカードの処理のフローチャート



【図１２】

第３の実施例の本体装置の処理のフローチャート



EXTERNAL VIEWS SHOWING A IC CARD ACCORDING TO THE EMBODIMENT (8)

FIG. 1 【図1】

本実施形態のICカードの外観図

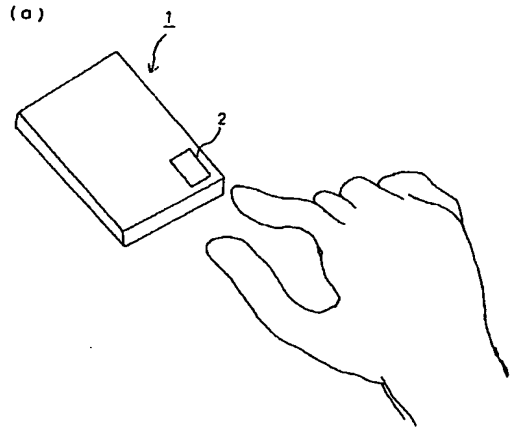
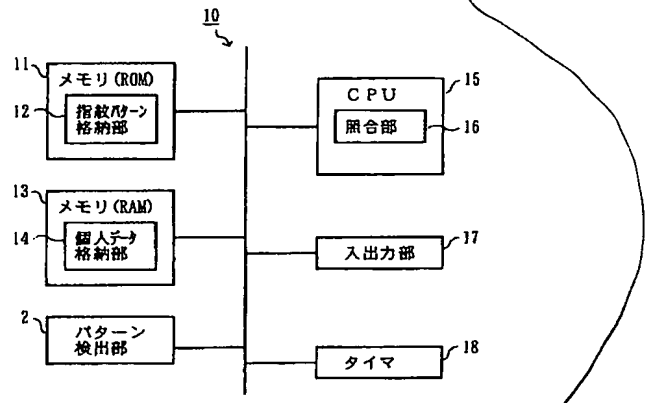


FIG. 2 【図2】

第1および第2の実施例のICカードの構成図



CONFIGURATION DIAGRAM OF THE IC CARD ACCORDING TO THE FIRST AND SECOND EMBODIMENT

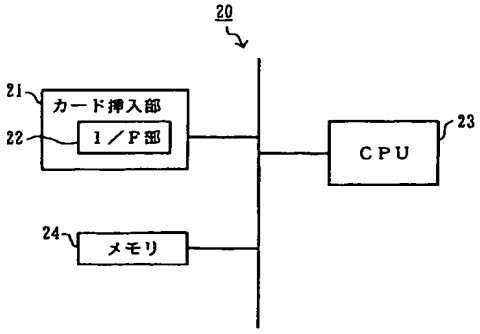
11 --- MEMORY
12 --- FINGERPRINT PATTERN STORING UNIT
13 --- MEMORY
14 --- PERSONAL DATA STORING UNIT
16 --- COMARING UNIT
17 --- INPUT/OUTPUT UNIT
18 --- TIMER
2 --- PATTERN DETECTOR

CONFIGURATION DIAGRAM OF THE MAIN APPARATUS ACCORDING TO THE FIRST AND SECOND EMBODIMENT

【図3】

FIG. 3

第1および第2の実施例の本体装置の構成図

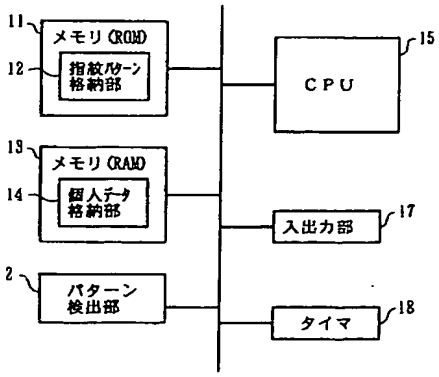


21 ··· CARD INSERTING UNIT
22 ··· I/F UNIT
24 ··· MEMORY

【図9】

FIG. 9

第3の実施例のICカードの構成図



FLOWCHART FOR THE IC CARD ACCORDING TO THE FIRST EMBODIMEN (1)

FIG.4 【図4】

第1の実施例のICカードの処理のフローチャート（その1）

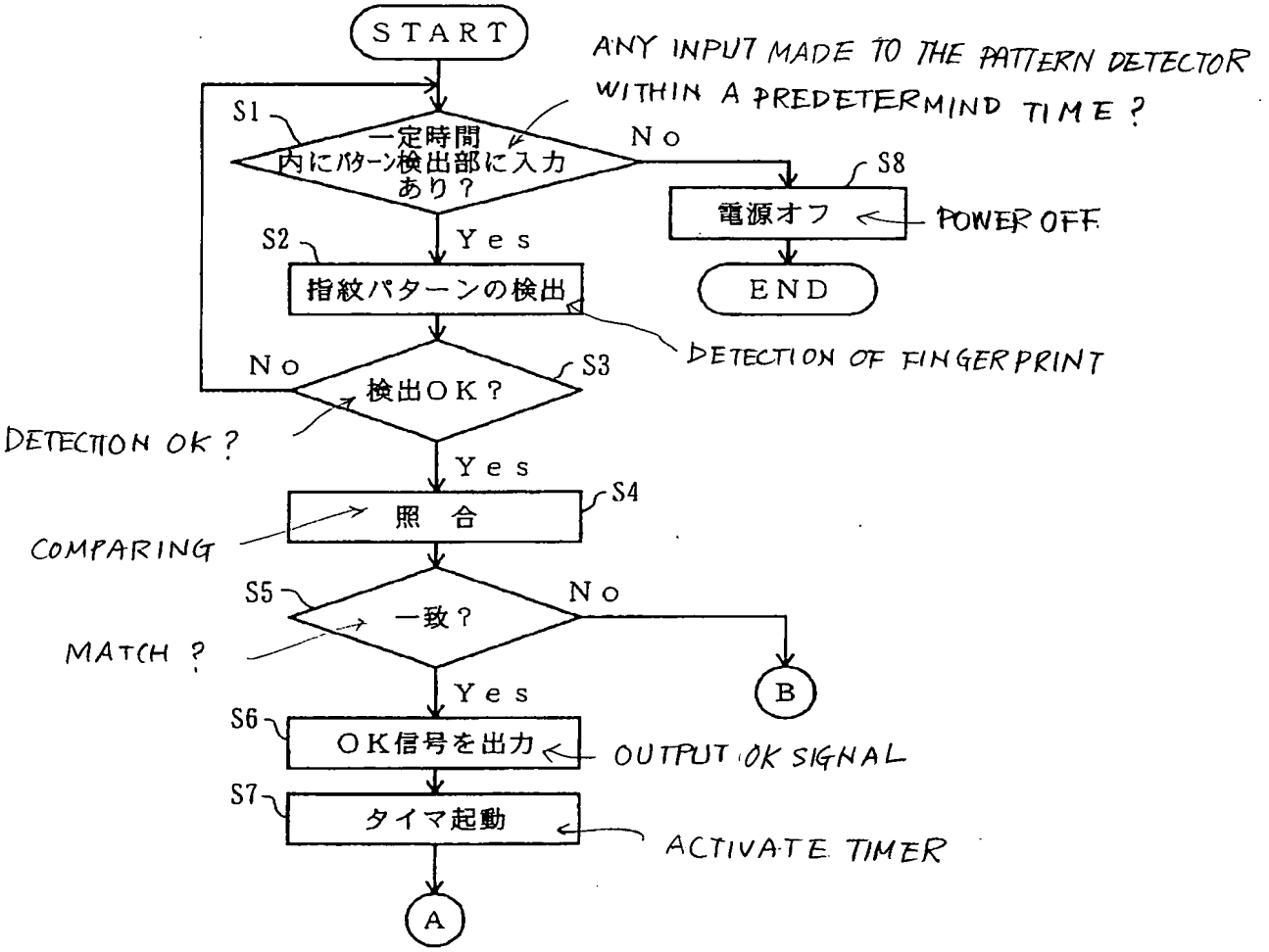
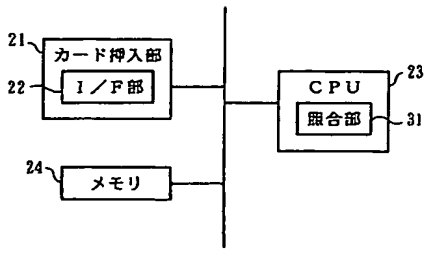


FIG.10

【図10】

第3の実施例の本体装置の構成図

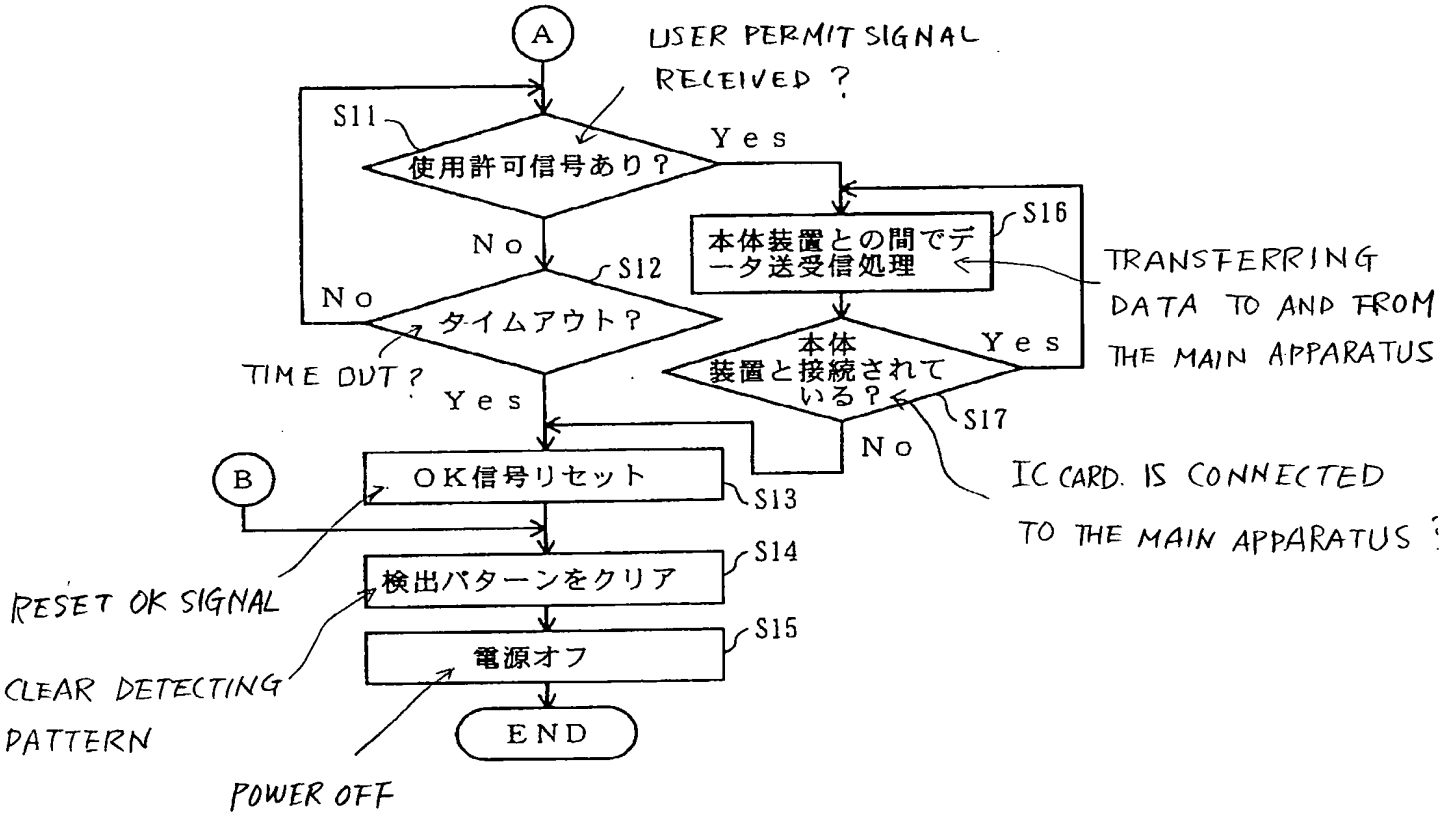


21 … CARD INSERTING UNIT
22 … I/F UNIT
24 … MEMORY
31 … COMPARING UNIT

FLOWCHART FOR THE IC CARD ACCORDING TO THE FIRST EMBODIMENT

FIG. 5 【図5】

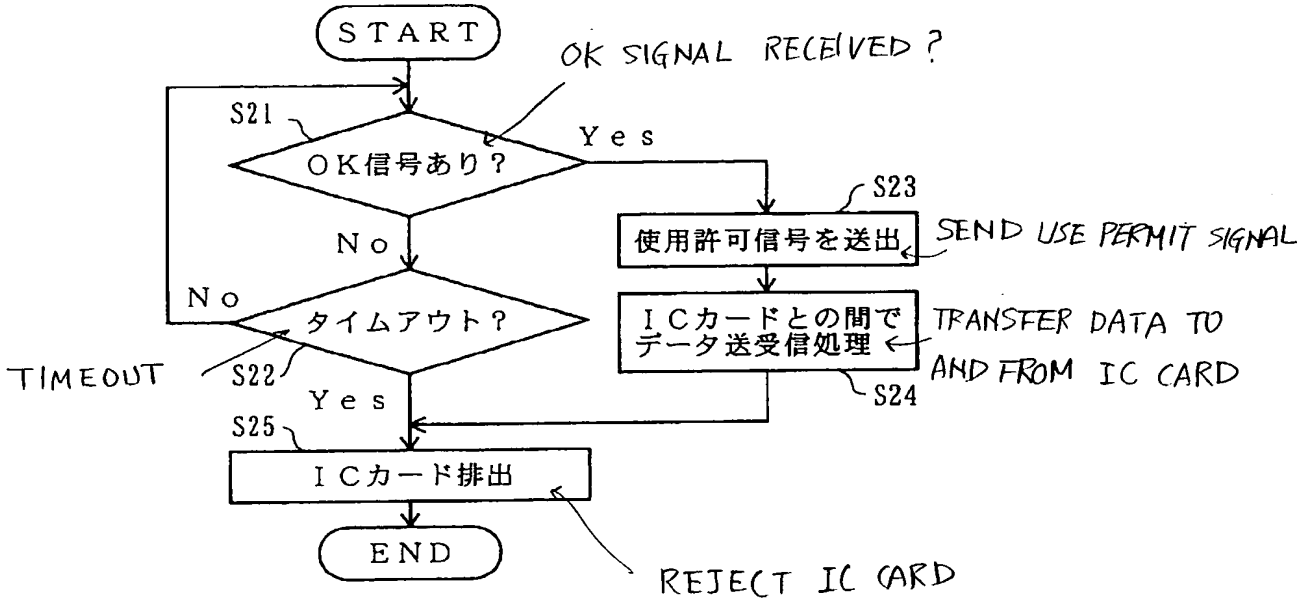
第1の実施例のICカードの処理のフローチャート（その2）



FLOWCHART FOR THE MAIN APPARATUS ACCORDING TO THE FIRST EMBODIMENT

FIG. 6 【図6】

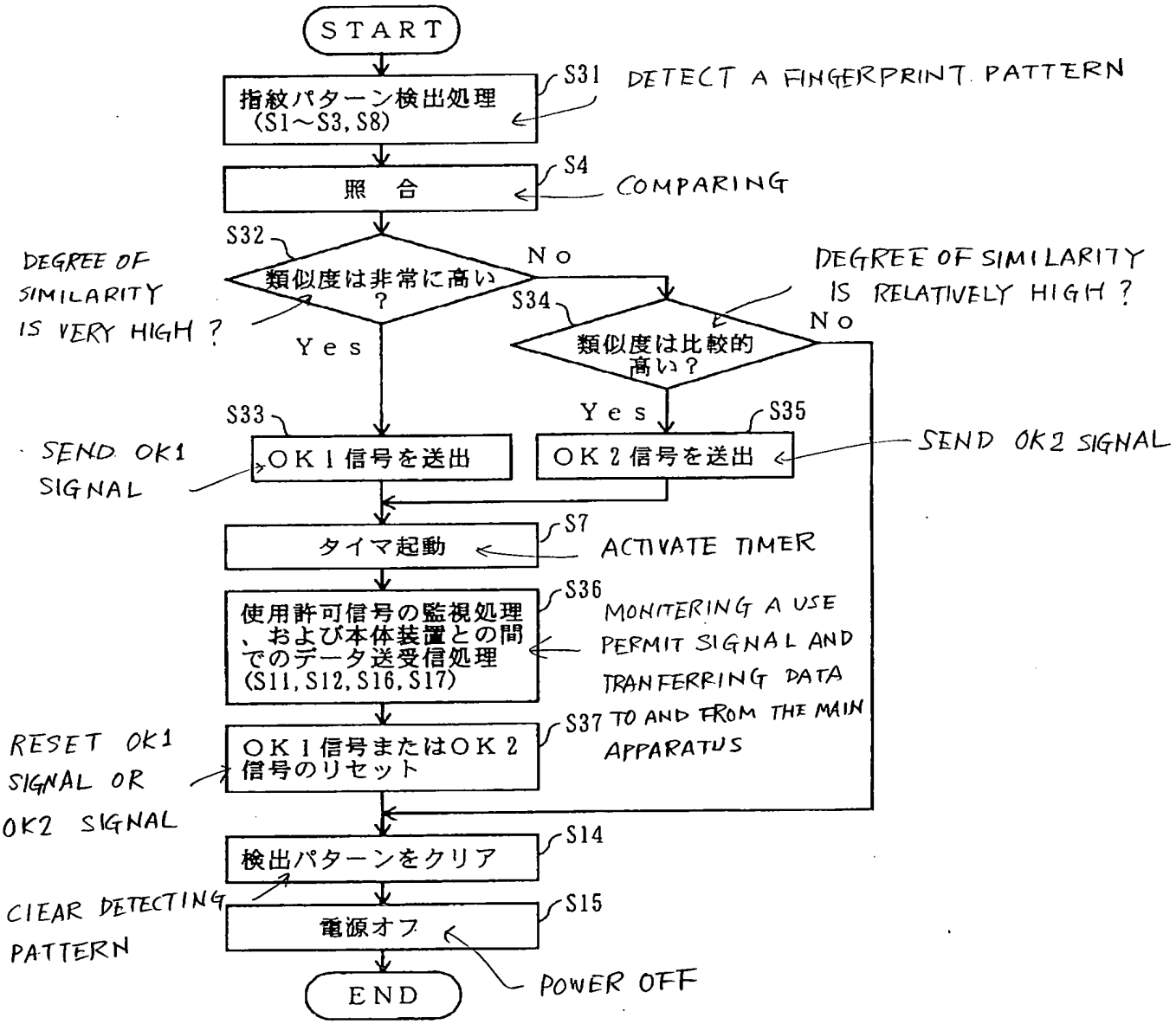
第1の実施例の本体装置の処理のフローチャート



FLOWCHART FOR THE IC CARD ACCORDING TO THE SECOND EMBODIMENT

FIG. 7 【図7】

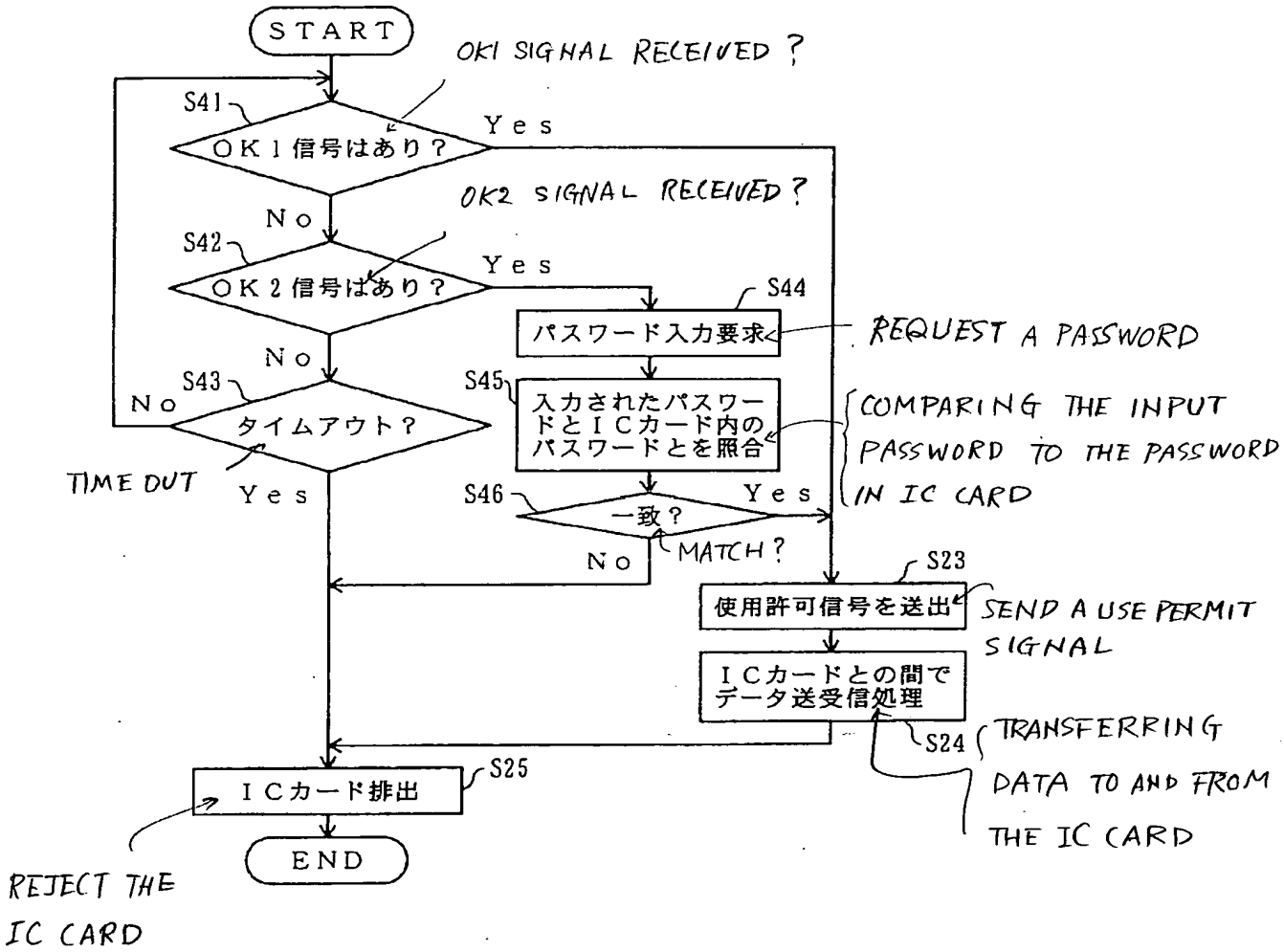
第2の実施例のICカードの処理のフローチャート



FLOWCHART FOR THE MAIN APPARATUS ACCORDING TO THE SECOND EMBODIMENT

FIG. 8 【図8】

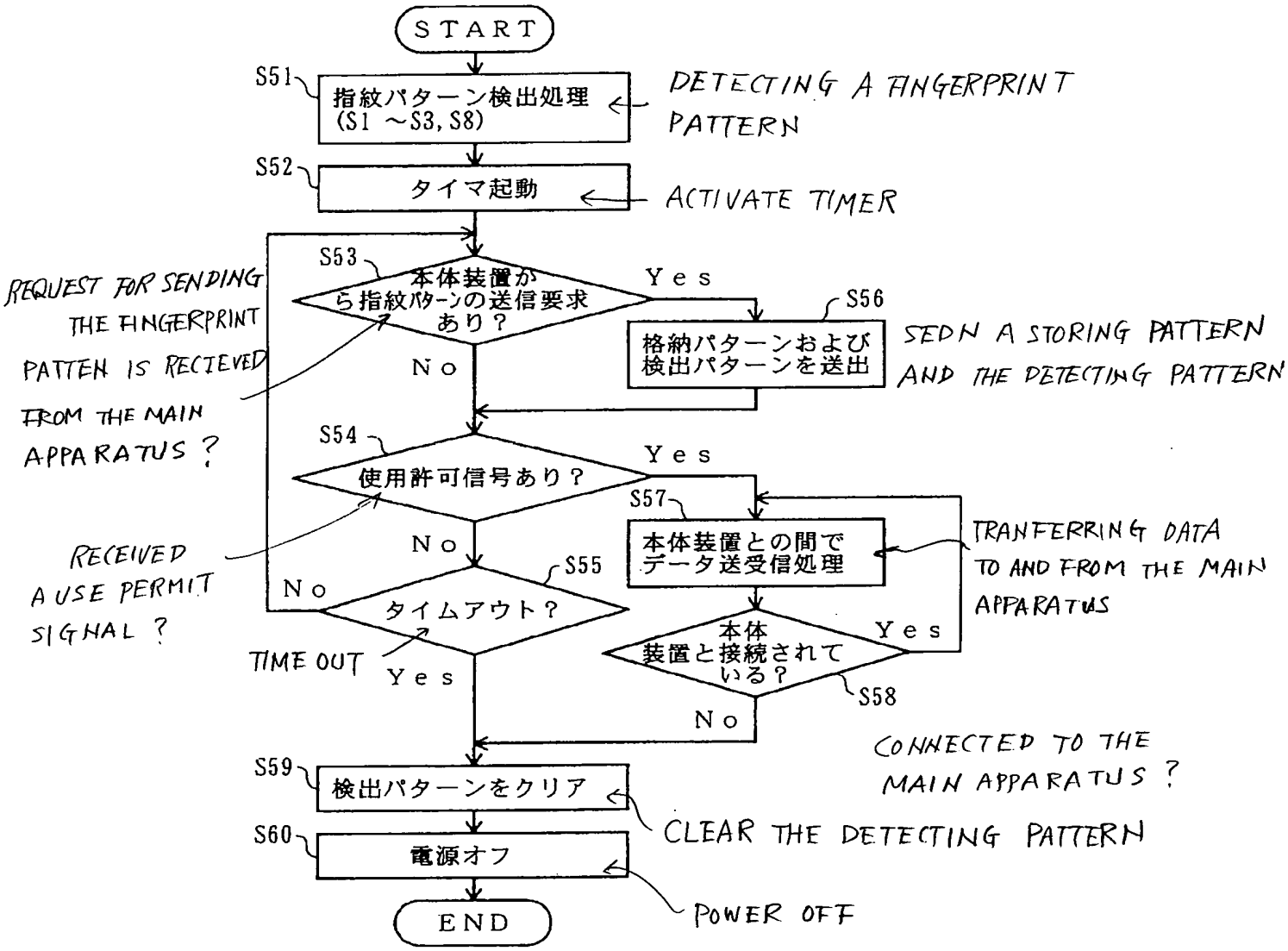
第2の実施例の本体装置の処理のフローチャート



FLOWCHART FOR THE IC CARD ACCORDING TO THIRD EMBODIMENT

FIG. 11 【図11】

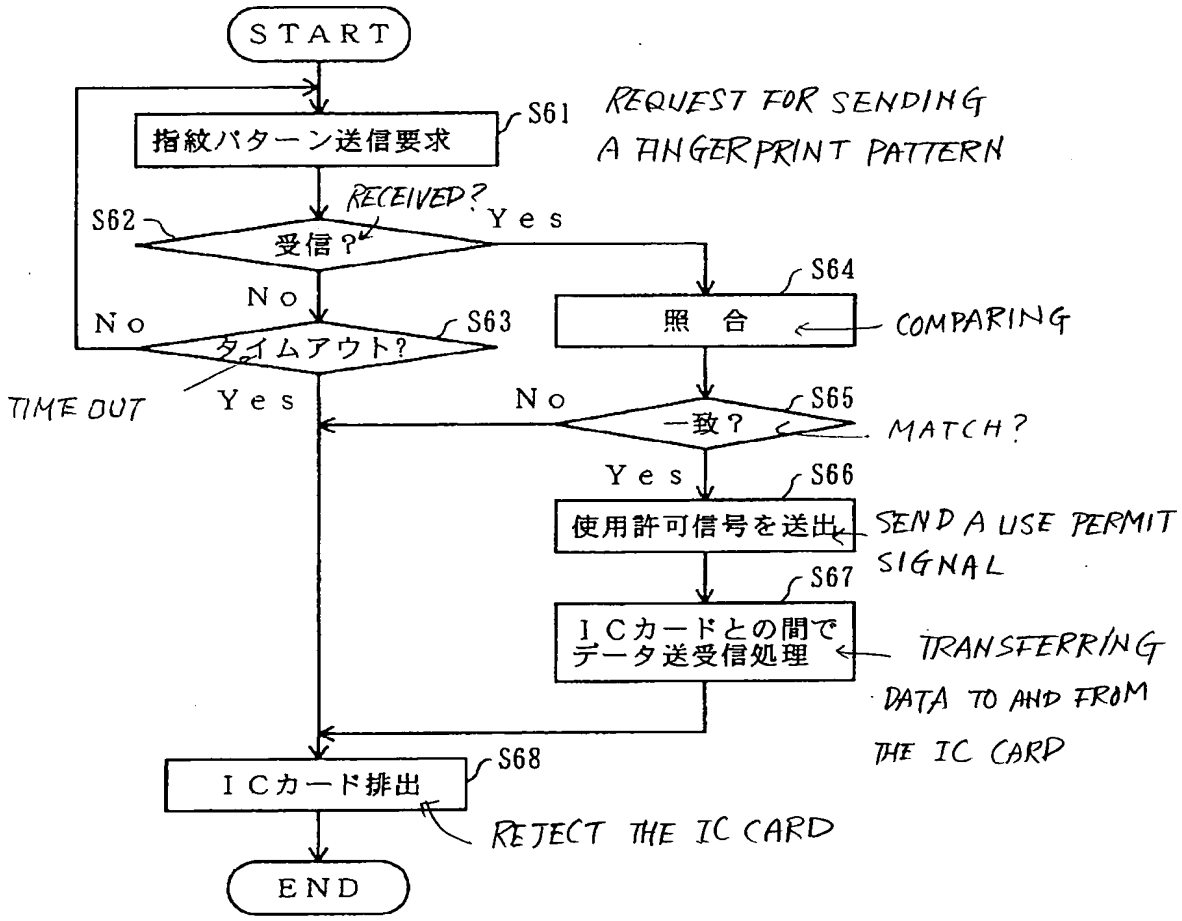
第3の実施例のICカードの処理のフローチャート



FLOWCHART FOR THE MAIN APPARATUS ACCORDING TO THE THIRD EMBODIMENT

FIG. 12 【図12】

第3の実施例の本体装置の処理のフローチャート



11-184992

[SCOPE OF CLAIMS]

[CLAIM 1] An IC card comprising:

detecting means for detecting a pattern on a surface of an object;

storing means for storing a fingerprint pattern; and

comparing means for comparing a fingerprint pattern detected by said detecting means against the fingerprint pattern stored in said storing means, and for outputting the result of said comparison, wherein

said IC card is inserted into an apparatus which, based on the result of said comparison output from said comparing means, makes a decision as to whether processing should be permitted or not.

[CLAIM 2] An IC card as claimed in claim 1, wherein said comparing means continues to output the result of said comparison for a predetermined period.

[CLAIM 3] An IC card comprising:

detecting means for detecting a pattern on a surface of an object;

storing means for storing a fingerprint pattern; and

output means for outputting a fingerprint pattern detected by said detecting means and the fingerprint pattern stored in said storing means, wherein

said IC card is inserted into an apparatus which compares said fingerprint patterns output from said output means and thereby makes a decision as to whether processing should be permitted or not.

[CLAIM 4] An apparatus into which an IC card is inserted, wherein said apparatus permits processing to be performed based on said IC card when a notification is received from said IC card notifying that a fingerprint pattern prestored in said IC card and a fingerprint pattern detected by said IC card have been found to match each other as a result of a comparison between said two fingerprint patterns.

[CLAIM 5] An apparatus as claimed in claim 4, wherein

when a result obtained by evaluating the degree of similarity between said two fingerprint patterns based on a plurality of levels is output as the result of said comparison from said IC card, then depending on the degree of similarity said apparatus permits processing to be performed based on said IC card, or requests a user password and permits processing to be performed based on said IC card when a legitimate password has been entered in response to said request, or prohibits processing to be performed based on said IC card.

[CLAIM 6] An apparatus into which an IC card is inserted, comprising:

receiving means for receiving from said IC card a fingerprint pattern prestored in said IC card and a fingerprint pattern detected by said IC card; and

comparing means for comparing said two fingerprint patterns, and for permitting processing to be performed based on said IC card when said fingerprint patterns match each other.

[CLAIM 7] An apparatus as claimed in claim 6, wherein said comparing means evaluates the degree of similarity between said two fingerprint patterns using a plurality of levels and, depending on the degree of similarity, permits processing to be performed based on said IC card, or requests a user password and permits processing to be performed based on said IC card when a legitimate password has been entered in response to said request, or prohibits processing to be performed based on said IC card.

[Problem to be solved by the invention] Currently, passwords are the most commonly used means to protect various kinds of cards (including IC cards) against illegal use by persons other than the authorized ones. Password protection, however, requires the user of each card to memorize the password; in particular, if the user has a large number of cards, the burden on the user increases. Furthermore, passwords carry the risk of leakage.

[0006] It is an object of the present invention to solve the

above problem and to provide an IC card and an apparatus into which the IC card is inserted, that can ensure high security while reducing the burden on the user side.

[Embodiments of the Invention] Embodiments of the present invention will be described below with reference to the drawings. Figures 1(a) and 1(b) are external views showing an IC card according to the embodiments of the invention. The IC card 1 is a card-type device used, for example, for accessing a bank account, for paying for purchased goods, for unlocking a door lock, or for activating various kinds of apparatuses. A pattern detector 2 is provided in a portion of the surface of the IC card 1. The pattern detector 2 has the function of detecting a surface pattern (ridge pattern, etc.) on an object contacted thereon, and is used in the embodiments of the invention to read the fingerprint pattern of a card user.

[0013] When using the IC card 1, the card user first turns a switch on, and then presses the predesignated finger onto the pattern detector 2. In the example shown in Figure 1(a), the user presses the index finger of his right hand onto the pattern detector 2. When pressing the predesignated finger onto the pattern detector 2, it is desirable to hold the IC card 1 between the index finger and the thumb (as shown in Figure 1(b)) so that the fingerprint pattern can be reliably detected.

[0014] The fingerprint pattern of the user's predesignated finger (in the example shown in Figure 1, the index finger of his right hand) is prestored in the IC card 1. In first and second embodiments hereinafter described, the IC card 1 compares the fingerprint pattern detected by the pattern detector 2 against the prestored fingerprint pattern, and outputs the result of the comparison. In a third embodiment, the IC card 1 outputs the prestored fingerprint pattern and the fingerprint pattern detected by the pattern detector 2 to the main apparatus into which the card has been inserted, and the main apparatus compares the fingerprint patterns. In

each embodiment, when the two fingerprint patterns match, the main apparatus permits processing (including an access using the IC card 1) to be performed based on the IC card 1, and thereafter data are transferred between them.

Embodiment 1

The first embodiment concerns a configuration in which the IC card is provided with the fingerprint matching function.

[0015] Figure 2 is a diagram showing the configuration of the IC card 10 according to the first (and second) embodiment. A memory 11 is a ROM area, and includes therein a fingerprint pattern storing part 12 in which the fingerprint pattern of the predesignated finger of the card user is stored. The fingerprint pattern is stored, for example, when the card is issued to the user. A program, etc. describing flowchart procedures to be described later is also stored in the memory 11. A memory 13 is a RAM area in which a personal data storing part 14 for storing personal information of the card user is provided in addition to an area used when executing the program. If the IC card 10 is, for example, an electronic wallet used in an electronic money system, the personal data storing part 14 stores such information as the "amount of money remaining in the wallet." The personal data storing part 14 is provided in a nonvolatile memory area.

[0016] The pattern detector 2 is a device for detecting ridges on the surface of an object pressed onto the detector surface, and is made thin enough to be incorporated into the IC card, which was made possible due to advances in miniaturization technology. The pattern detector 2 includes, for example, a light source and a two-dimensional photosensor, and a large number of light detecting elements forming the photosensor output in parallel or serial form the electric current values or voltage values corresponding to their respectively detected light levels. The applicant of the present invention previously filed a patent application for a reading device that is sufficiently thin and yet

capable of detecting a ridge pattern on the surface of an object with high accuracy (Japanese Patent Application No. H09-222018).

[0017] A CPU 15 executes the program stored in the memory 11. The CPU 15 includes a comparing part 16. The comparing part 16 is implemented by executing a portion of the program, and compares the card user's fingerprint pattern read by the pattern detector 2 against the fingerprint pattern stored in the fingerprint pattern storing part 12. An input/output part 17 transfers data to and from the main apparatus into which the IC card 10 has been inserted. A timer 18 is activated by the CPU 15, and sends an interrupt signal when a predetermined time has elapsed.

[0018] Figure 3 is a diagram showing the configuration of the main apparatus 20 according to the first (and second) embodiment. The IC card 10 shown in Figure 1 is inserted into this main apparatus 20. The IC card 10 is inserted into a card inserting part 21. The card inserting part 21 includes an I/F part 22 for interfacing with the IC card 10. By executing a program stored in a memory 24, a CPU 23 controls data transfers to and from the IC card 10 and, if needed, data transfers to and from an external device (such as a host computer) not shown. The memory 24 stores various kinds of data that the main apparatus 20 uses, as well as programs describing flowchart procedures hereinafter described and other software processing of the main apparatus 20. In the example shown here, the card inserting part 21, the CPU 23, and the memory 24 are provided within the same apparatus, but alternatively, these may be provided at separate locations and interconnected via communication lines or the like.

[0019] Figures 4 and 5 show a processing flowchart for the IC card according to the first embodiment. The process shown here is initiated when power is turned on to the IC card.

[0020] In step S1, it is checked whether any input has been made to the pattern detector 2 within a predetermined time after turning the power on. This processing is performed,

for example, to check whether the output of the pattern detector 2 has changed or not. When an input has been made to the pattern detector 2, the process proceeds to step S2 by determining that the user has pressed the tip portion of his predesignated finger (the portion where the fingerprint is formed) onto the pattern detector 2; on the other hand, when there is no input, the power of the IC card is turned off in step S8.

[0021] In step S2, the fingerprint pattern is detected. That is, the output of the pattern detector 2 is captured. The detected fingerprint pattern is stored, for example, into a designated area in the memory 13. In step S3, it is determined whether the fingerprint pattern has been properly detected. That is, the fingerprint pattern cannot be reproduced, for example, if the user's finger has not been held fixed on the pattern detector 2 for more than a certain length of time or has not been pressed firmly enough to produce a sufficient contact area; therefore, a decision is made in this step as to whether the fingerprint pattern has been properly detected or not. If the fingerprint pattern has been properly detected, the process proceeds to step S4, but if it has not been detected, the process returns to step S1.

[0022] In step S4, the fingerprint pattern detected by the pattern detector 2 is compared against the fingerprint pattern stored in the fingerprint pattern storing part 12. This processing involves, for example, converting the degree of similarity between the two fingerprint patterns into a numerical value.

[0023] In step S5, whether the patterns match or do not match is determined by checking whether or not the value representing the degree of similarity obtained in step S4 is greater than a predetermined threshold value. If the two fingerprint patterns match, an OK signal is output in step S6. This processing is accomplished, for example, by changing from "L" level to "H" level a predetermined one of the terminals contacting the I/F part 22 of the main

apparatus 20 into which the IC card has been inserted. In step S7, the timer 18 is activated.

[0024] In steps S11 and S12, it is checked whether or not a use permit signal has been received. As will be described later, the use permit signal is a signal generated by the main apparatus 20 shown in Figure 4, and is output from the main apparatus 20 when a decision is made by the main apparatus 20 to permit the processing to be performed based on the IC card inserted therein. Here, when the use permit signal has been received before the expiration of the time preset by the timer 18, processing for transferring data to and from the main apparatus 20 is performed in steps S16 and S17. This processing continues as long as the IC card remains connected to the main apparatus 20.

[0025] When the IC card is disconnected from the main apparatus 20, for example, by ejecting the IC card out of the main apparatus 20, the process proceeds to step S13 to reset the OK signal. That is, the transmission of the OK signal is stopped. Next, in step S14, the fingerprint pattern detected in step S2 by the pattern detector 2 is cleared. Finally, in step S15, the power of the IC card is turned off.

[0026] On the other hand, if, in steps S11 and S12, the use permit signal has not been received before the expiration of the time preset by the timer 18, that is, if the timer 18 has timed out, the process proceeds to step S13 by skipping steps S16 and 17. That is, if the permit signal from the main apparatus 20 has not been received, the IC card cannot transmit or receive data to or from the main apparatus 20.

[0027] If, in step S5, it is determined that the fingerprint pattern detected by the pattern detector 2 does not match the fingerprint pattern stored in the fingerprint pattern storing part 12, the process jumps to step S14 without outputting the OK signal, and power is turned off after clearing the detected fingerprint pattern.

[0028] Figure 6 is a processing flowchart for the main apparatus according to the first embodiment. The process shown here is initiated when the IC card 10 is inserted. In

steps S21 and S22, it is checked whether an OK signal has been received from the IC card 10 within a predetermined time after the insertion of the IC card 10. As previously described, the OK signal is output from the IC card 10 when the fingerprint pattern detected by the pattern detector 2 matches the fingerprint pattern stored in the fingerprint pattern storing part 12. If the OK signal has been received, the process proceeds to step S23; on the other hand, if the OK signal has not been received, the inserted IC card 10 is ejected in step S25.

[0029] In step S23, a use permit signal is sent to the IC card 10. The use permit signal is a signal that is monitored in steps S11 and S12 in Figure 5; when this signal is received, the IC card 10 is enabled to transfer data to and from the main apparatus. In step S24, processing is performed to transfer data to and from the IC card 10. Here, since the OK signal earlier received is information that indicates whether the person whose fingerprint has been read by the IC card is the authorized user (holder) of the IC card, information identifying the user of the IC card is received in step S24. Accordingly, in such cases as where the information identifying the user of the IC card is not legally registered, the processing based on the IC card may not be permitted even when the OK signal has been received. Further, if there is a need to transfer data to and from a host computer or the like not shown when the main apparatus performs data transfer to and from the IC card 10, the processing is performed concurrently with the processing of step S24.

[0030] As described above, in the first embodiment, the IC card makes a decision by itself as to whether the person trying to use the IC card is the authorized user or not, and notifies the main apparatus of the result of the decision. If any person other than the authorized user is trying to use the IC card (unauthorized use), the main apparatus prohibits the processing to be performed based on the IC card.

Embodiment 2

The configuration of the second embodiment is substantially the same as that of the first embodiment, the only difference being the inclusion of a mechanism that requests a password from the user when it is not possible to clearly determine whether the fingerprint patterns match or not. The IC card and the main apparatus in the second embodiment are identical in configuration to those in the first embodiment shown in Figures 2 and 3, respectively.

[0031] Despite recent advances in image recognition technology, the accuracy of pattern matching is generally not 100 percent. The accuracy will drop further when the capability of the processor is low or in a situation where the processing has to be done in a short time. Accordingly, it is realistic to determine whether the person trying to use the IC card is the authorized user or not, by checking whether or not the numerical value representing the degree of fingerprint pattern similarity is greater than the predetermined threshold value as described in the first embodiment. However, it is difficult to set the threshold value; if the match/nonmatch criterion is loosened, it will run the risk of being unable to reject unauthorized use, and conversely, if the criterion is tightened, there can occur cases where, even when the authorized user is accessing, the access may not be granted.

[0032] In view of this, in the second embodiment, the IC card evaluates the degree of fingerprint pattern similarity using a plurality of levels so that a more accurate determination can be made when determining whether the processing based on the IC card should be permitted or not. More specifically, the degree of fingerprint pattern similarity is evaluated using three levels, "very high", "relatively high", and "low", and when the evaluation "similarity very high" is received, the main apparatus permits the processing at once, but when the evaluation "similarity relatively high" is received, the main apparatus requests the user to enter a password.

[0033] Figure 7 is a processing flowchart for the IC card

according to the second embodiment. The process shown here, as in the first embodiment, is initiated when power is turned on to the IC card. In Figure 7, the comparing step (step S7), the timer activating step (step S7), the clearing step (step S14), and the power off step (step S15) are the same as those in the first embodiment.

[0034] In step S31, the fingerprint pattern is detected by the pattern detector 2. This processing is the same as that performed in steps S1 to S3 and S8 in the first embodiment. Next, in step S4, the fingerprint pattern detected by the pattern detector 2 is compared against the fingerprint pattern stored in the fingerprint pattern storing part 12, and the degree of similarity between them is converted into a numerical value.

[0035] In step S32, it is checked whether the degree of similarity obtained in step S4 is "very high" or not. If the degree of similarity is very high, an OK1 signal is output in step S33; otherwise, the process proceeds to step S34. In step S34, it is checked whether the degree of similarity obtained in step S4 is "relatively high" or not. If the degree of similarity is relatively high, an OK2 signal is output in step S35. When the OK1 or OK2 signal is output, the timer 18 is activated in step S7.

[0036] Step S36 performs the processing for monitoring for the use permit signal and the processing for transferring data to and from the main apparatus when the use permit signal is received. The details of the processing are the same as those of the processing performed in steps S11, S12, S16, and S17 in the first embodiment. In step S37, the OK1 or OK2 signal is reset. That is, the output of the OK1 or OK2 signal is stopped. The processing for resetting these signals is performed when the timer 18 has timed out or when the use permit signal is received from the main apparatus. After that, in steps S14 and S15, the pattern detected by the pattern detector 2 is cleared, and the power of the IC card is turned off.

[0037] On the other hand, if it is determined that the

degree of similarity obtained in step S4 is low (step S32: No, and step S34: No), then it is determined that a person other than the authorized user is trying to use the IC card, and the process jumps to step S14 without outputting the OK1 signal or the OK2 signal.

[0038] Figure 8 is a processing flowchart for the main apparatus according to the second embodiment. The process shown here, as in the first embodiment, is initiated when the IC card is inserted.

[0039] Steps S41 to S43 are steps for monitoring whether the OK1 signal or the OK2 signal is received from the inserted IC card within a predetermined time. When the OK1 signal is received, that is, when it is notified that the degree of similarity between the two fingerprint patterns compared in the IC card is very high, the use permit signal is sent out in step S23 by determining that the person trying to use the IC card is the authorized user. Then, in step S24, the processing for transferring data to and from the IC card is performed. These steps S23 and S24 are the same as the corresponding steps in the first embodiment.

[0040] When the OK2 signal is received, that is, when it is notified that the degree of similarity between the two fingerprint patterns compared in the IC card is relatively high, it is highly likely that the person trying to use the IC card is the authorized user, but there is the possibility that the person may not be the authorized user; therefore, a password is requested in step S44. Next, in step S45, information identifying the inserted IC card is read from the IC card, and the preregistered password that matches the identifying information is extracted. Then, the password that the card user entered in response to the above request is compared with the preregistered password. In step S46, the result of the comparison in step S45 is checked, and if the passwords match, the process proceeds to step S23 to perform the processing for transmitting the use permit signal and the processing for transferring data to and from the IC card; on the other hand, if they do not match, the process

proceeds to step S25 by skipping the above processing.

[0041] If neither the OK1 signal nor the OK2 signal has been received within the predetermined time, it is determined that the person trying to use the IC card is not the authorized user, and the IC card is ejected without sending the use permit signal.

[0042] As described above, in the second embodiment, a mechanism has been incorporated that requests a password from the user when, from the result of the comparison of the fingerprint patterns alone, it is not possible to determine whether the person trying to use the IC card is the authorized user or not. This reliably rejects unauthorized users who do not know the correct password, while avoiding the situation where the authorized user becomes unable to use the IC card. Furthermore, since the password is used in combination with the fingerprint, even when the accuracy of fingerprint pattern matching is not very high, it can be determined whether the person trying to use the IC card is the authorized user or not. Accordingly, the capability of the CPU provided within the IC card need not be very high, and this serves to suppress the increase in the cost of the IC card itself.

Embodiment 3

The third embodiment concerns a configuration in which the processing for fingerprint pattern matching is performed in the main apparatus in which the IC card is inserted.

[0043] Figure 9 is a diagram showing the configuration of the IC card according to the third embodiment. The configuration of the IC card in the third embodiment is basically the same as that in the first or second embodiment, but the comparing part 16 is not included because the fingerprint pattern matching is not performed here.

[0044] Figure 10 is a diagram showing the configuration of the main apparatus according to the third embodiment. The configuration of the main apparatus in the third embodiment is basically the same as that in the first or second embodiment, except that the main apparatus here performs the

fingerprint pattern matching. For this purpose, the CPU 31 includes a comparing part 31 which is one of the functions implemented by executing the program stored in the memory 24.

[0045] Figure 11 is a processing flowchart for the IC card according to the third embodiment. The process shown here, as in the first or second embodiment, is initiated when power is turned on to the IC card.

[0046] In step S51, the fingerprint pattern is detected by the pattern detector 2. This processing is the same as that performed in steps S1 to S3 and S8 in the first embodiment. Next, in step S52, the timer 18 is activated.

[0047] In steps S53 to S55, it is checked whether or not a fingerprint transmit request has been received from the main apparatus in which the IC card is inserted, and whether or not a use permit signal has been received from the main apparatus before the expiration of the timer 18. When the fingerprint transmit request is received from the main apparatus, the fingerprint pattern stored in the fingerprint pattern storing part 12 and the fingerprint pattern detected by the pattern detector 2 are transmitted in step S56 to the main apparatus. When the use permit signal is received, processing for transferring data to and from the main apparatus is performed in steps S57 and S58. This processing continues as long as the IC card remains connected to the main apparatus.

[0048] If the timer 18 has timed out before the use permit signal is received from the main apparatus, or if the IC card is disconnected from the main apparatus, the pattern detected by the pattern detector 2 is cleared in step S59, and the power of the IC card is turned off in step S60.

[0049] As described above, the IC card of the third embodiment transmits the prestored fingerprint pattern and the detected fingerprint pattern in response to the request received from the main apparatus. Based on these fingerprint patterns, the main apparatus makes a decision as to whether the use should be permitted or not. Only when the use permit is given from the main apparatus, can the IC card initiate

data transfer to and from the main apparatus.

[0050] Figure 12 is a processing flowchart for the main apparatus according to the third embodiment. The process shown here, as in the first or second embodiment, is initiated when the IC card is inserted.

[0051] In steps S61 to S63, a request is made to the inserted IC card to output the fingerprint patterns, and it is checked whether the fingerprint patterns can be received within a predetermined time in response to the request. When the fingerprint patterns have been received from the IC card, the process proceeds to step S64; otherwise, the process proceeds to step S68 where the IC card is ejected.

[0052] In step S64, the two fingerprint patterns received from the IC card, that is, the fingerprint pattern stored in the fingerprint pattern storing part 12 and the fingerprint pattern detected by the pattern detector 2, are compared with each other. This processing is, for example, the same as that performed in step S4 in Figure 4, and involves converting the degree of similarity between them into a numerical value. In step S65, by referring to the result of the comparison in step S64, a decision is made as to whether or not the two fingerprints match. If they match, the use permit signal is sent to the IC card in step S66, and data transfer to and from the IC card is performed in step S67. On the other hand, if the two fingerprints do not match, the process skips steps S66 and S67 and proceeds to step S68 where the IC card is ejected.

[0053] As described above, the main apparatus of the third embodiment receives the prestored fingerprint pattern and the detected fingerprint pattern from the IC card inserted therein, and gives the use permit to the IC card only when the fingerprint patterns match.

[0054] In the third embodiment also, the fingerprint pattern matching may be combined with password authentication as in the foregoing second embodiment. In the third embodiment, as the fingerprint pattern matching is not performed in the IC card, as described above, the CPU provided within the IC card

need not have high performance. This contributes to reducing the manufacturing cost of the IC card.

[0055] The first to third embodiments described above have each shown the configuration in which the fingerprint pattern of a single user is prestored in each IC card, but it will be appreciated that the present invention is not limited to this particular configuration. For example, provisions may be made so that the same IC card can be shared among family members or among a particular group of people. In that case, the fingerprint patterns of a plurality of persons are preregistered in the IC card, and the detected fingerprint pattern is compared against the plurality of preregistered fingerprint patterns.

[0056]

[Advantageous Effect of the Invention] High security is achieved because the decision as to whether the person trying to use the IC card is the authorized user or not is made based on fingerprint patterns. At this time, the card user need not memorize the password or the like as in the prior art system, and there is therefore no risk of leakage of the password, etc. Furthermore, the IC card can be used by simple operation.